Fortinet.NSE7_OTS-7.2.v2024-02-05.q24

Exam Code:	NSE7_OTS-7.2
Exam Name:	Fortinet NSE 7 - OT Security 7.2
Certification Provider:	Fortinet
Free Question Number:	24
Version:	v2024-02-05
# of views:	1141
# of Questions views:	240
https://www.freepdfdumps.com/Fortinet.NSE7_OTS-7.2.v2024-02-05.q24.html	

NEW QUESTION: 1
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?
A. A FortiSIEM CMDB report
B. A FortiSIEM analytics report
C. A FortiSIEM incident report
D. A FortiAnalyzer device report
Answer: (SHOW ANSWER)

NEW QUESTION: 2
Refer to the exhibit.

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

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

A. FortiGate is configured with forward-domains to forward only domain controller traffic.

B. FortiGate is configured with forward-domains to reduce unnecessary traffic.

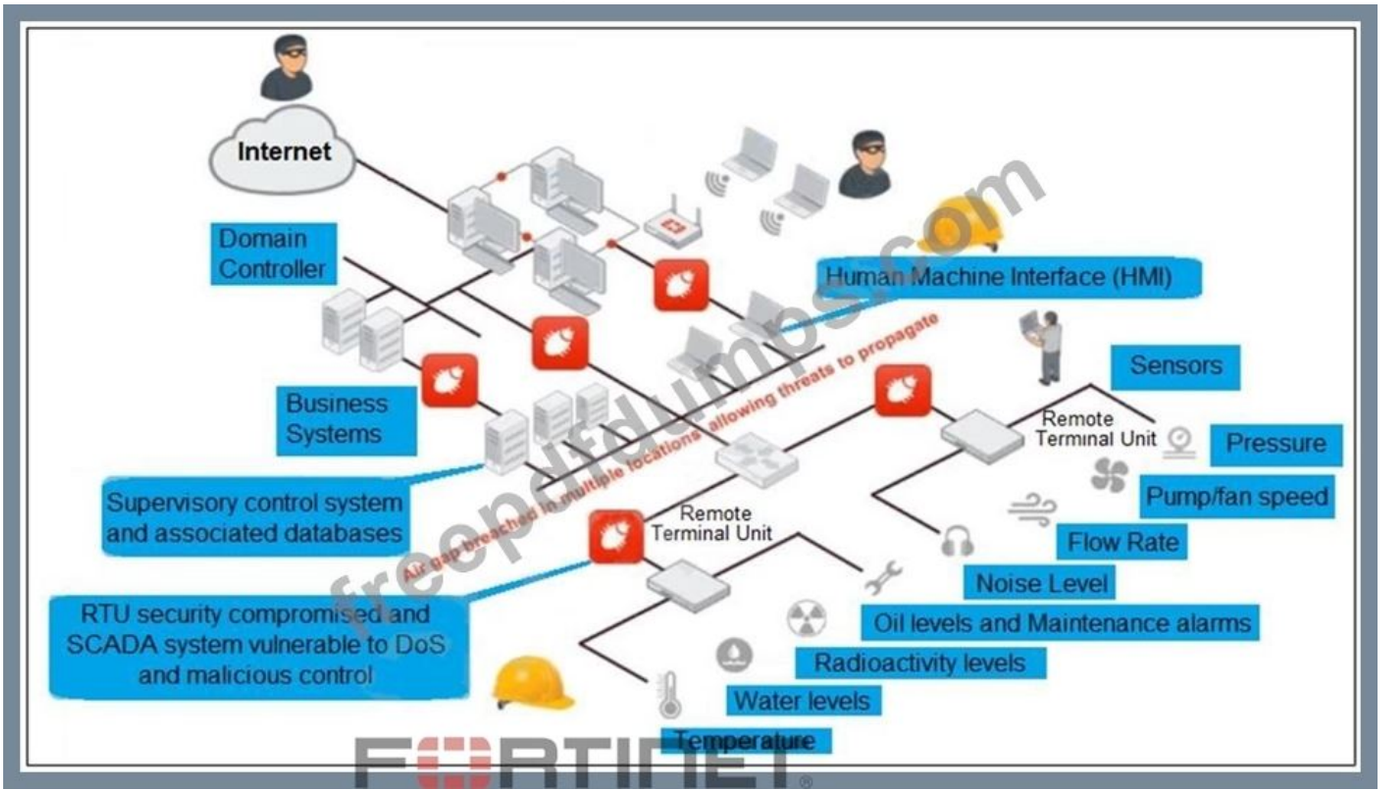
C. FortiGate is configured with forward-domains to filter and drop non-domain controller traffic.

D. FortiGate is configured with forward-domains to forward only company domain website traffic.

Answer: (SHOW ANSWER)

NEW QUESTION: 3

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. Configure firewall policies with industrial protocol sensors

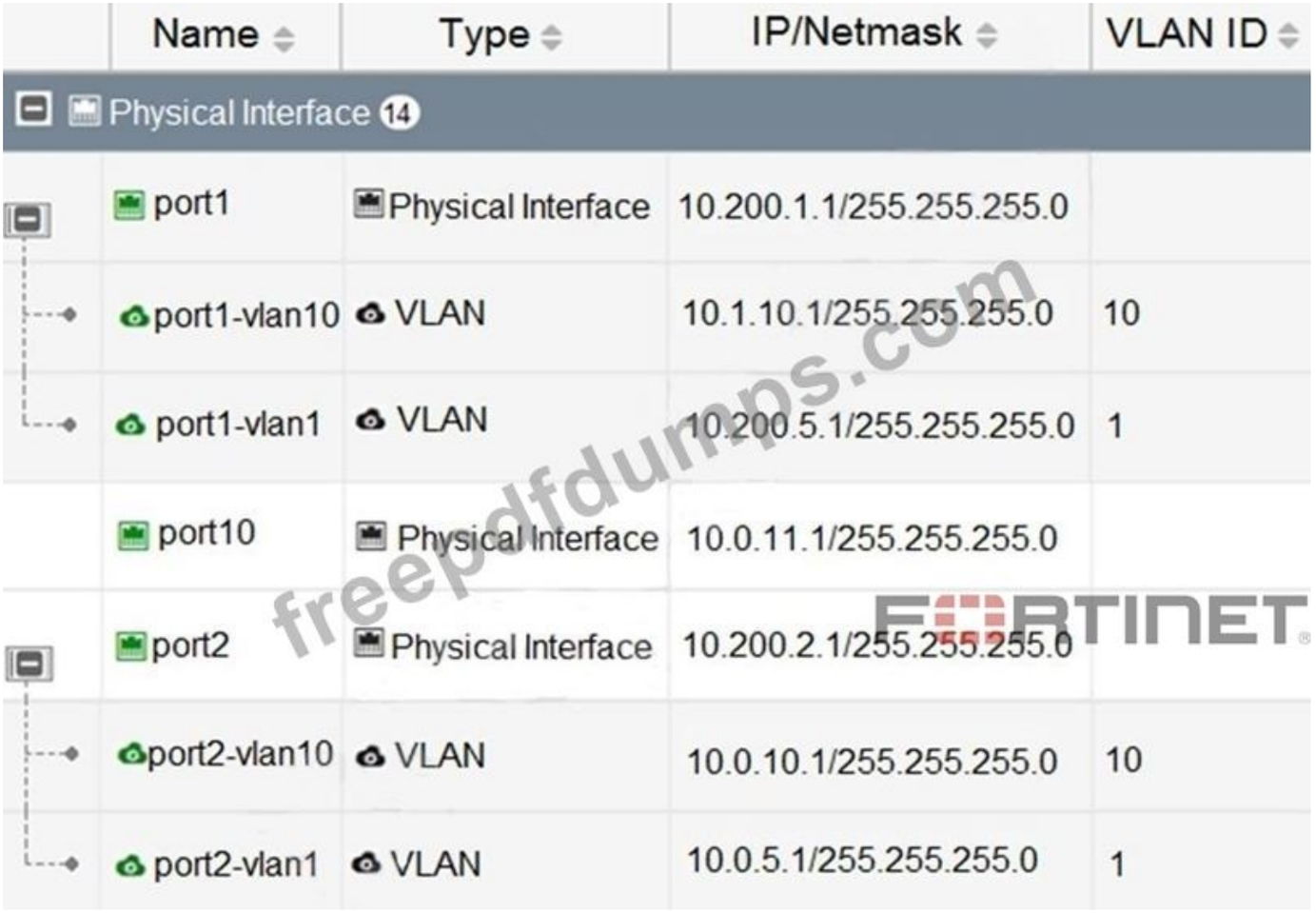
B. Configure firewall policies with web filter to protect the different ICS networks.

C. Use segmentation
D. Deploy an edge FortiGate between the internet and an OT network as a one-arm sniffer.
E. Deploy a FortiGate device within each ICS network.
Answer: A,B,D (LEAVE A REPLY)

NEW QUESTION: 4
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: (SHOW ANSWER)
Explanation
https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/32cb817d-a307-11eb-b70b-0050569258

NEW QUESTION: 5
What triggers Layer 2 polling of infrastructure devices connected in the network?
A. A matched profiling rule
B. A failed Layer 3 poll
C. A matched security policy
D. A linkup or linkdown trap
Answer: (SHOW ANSWER)

NEW QUESTION: 6
Refer to the exhibit.



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

A. port1, port1-vlan10, and port1-vlan1 are in different broadcast domains

B. The VLAN ID of port1-vlan1 can be changed to the VLAN ID 10.

C. port2, port2-vlan10, and port2-vlan1 are part of the software switch interface.

D. port1-vlan10 and port2-vlan10 are part of the same broadcast domain

Answer: A (LEAVE A REPLY)

NEW QUESTION: 7

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. Application control

D. Antivirus inspection

Answer: (SHOW ANSWER)

NEW QUESTION: 8

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

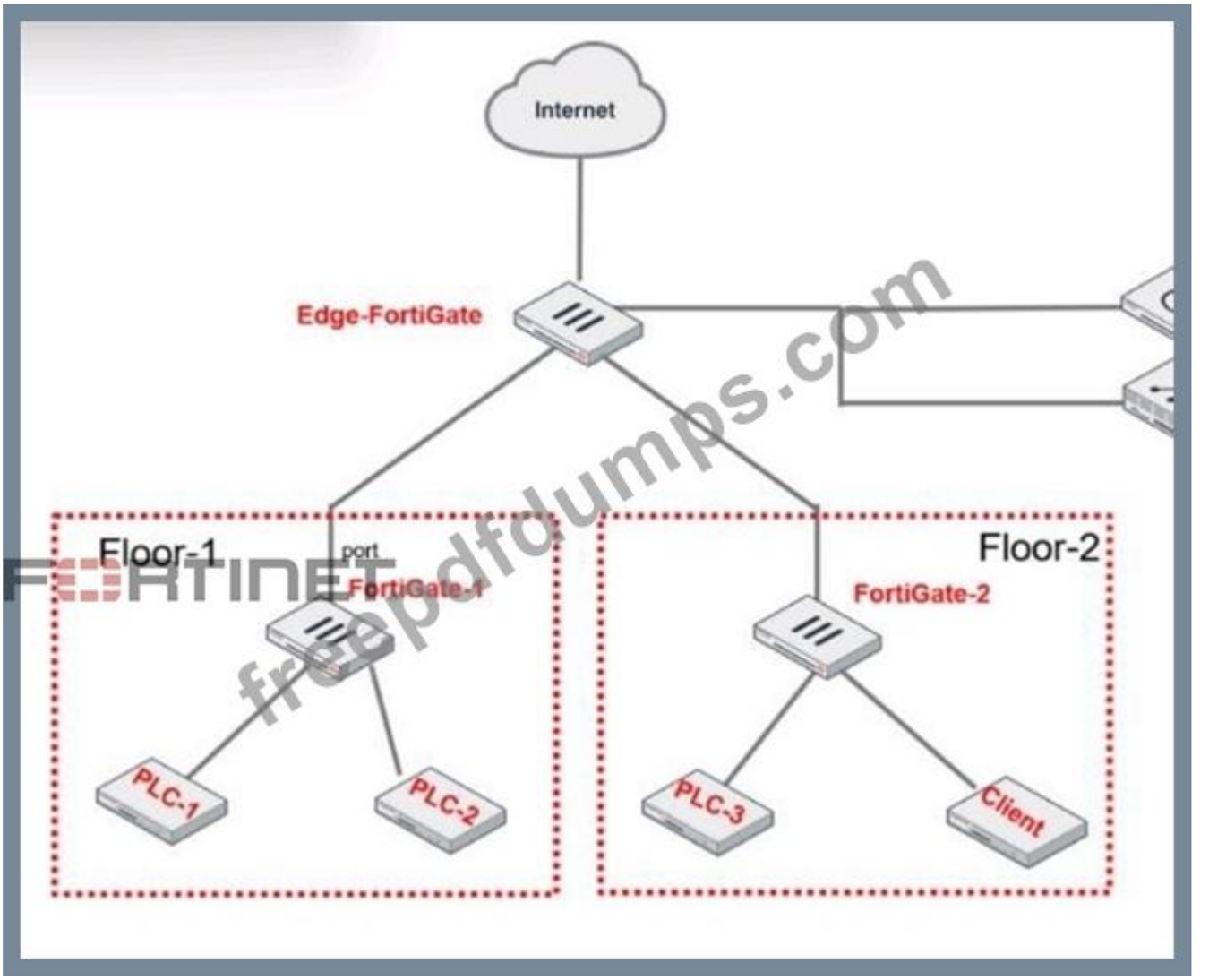
A. Importation and classification of hosts

B. Direct VLAN assignment
C. Adapter consolidation for multi-adapter hosts
D. Enhanced point of connection details
Answer: (SHOW ANSWER)

NEW QUESTION: 9
How can you achieve remote access and internel availability in an OT network?
A. Add additional internal firewalls to access OT devices.
B. Implement SD-WAN to manage traffic on each ISP link.
C. Create a back-end backup network as a redundancy measure.
D. Create more access policies to prevent unauthorized access.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 10
Which three methods of communication are used by FortiNAC to gather visibility information? (Choose three.)
A. ICMP
B. API
C. SNMP
D. RADIUS
E. TACACS
Answer: (SHOW ANSWER)

NEW QUESTION: 11
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. Enable explicit intra-switch policy to require firewall policies on FGT-2.

B. Create a VLAN for each device and replace the current FGT-2 software switch members.

C. Set a unique forward domain for each interface of the software switch.

D. Implement policy routes on FGT-2 to control traffic between devices.

Answer: B,C (LEAVE A REPLY)

NEW QUESTION: 12

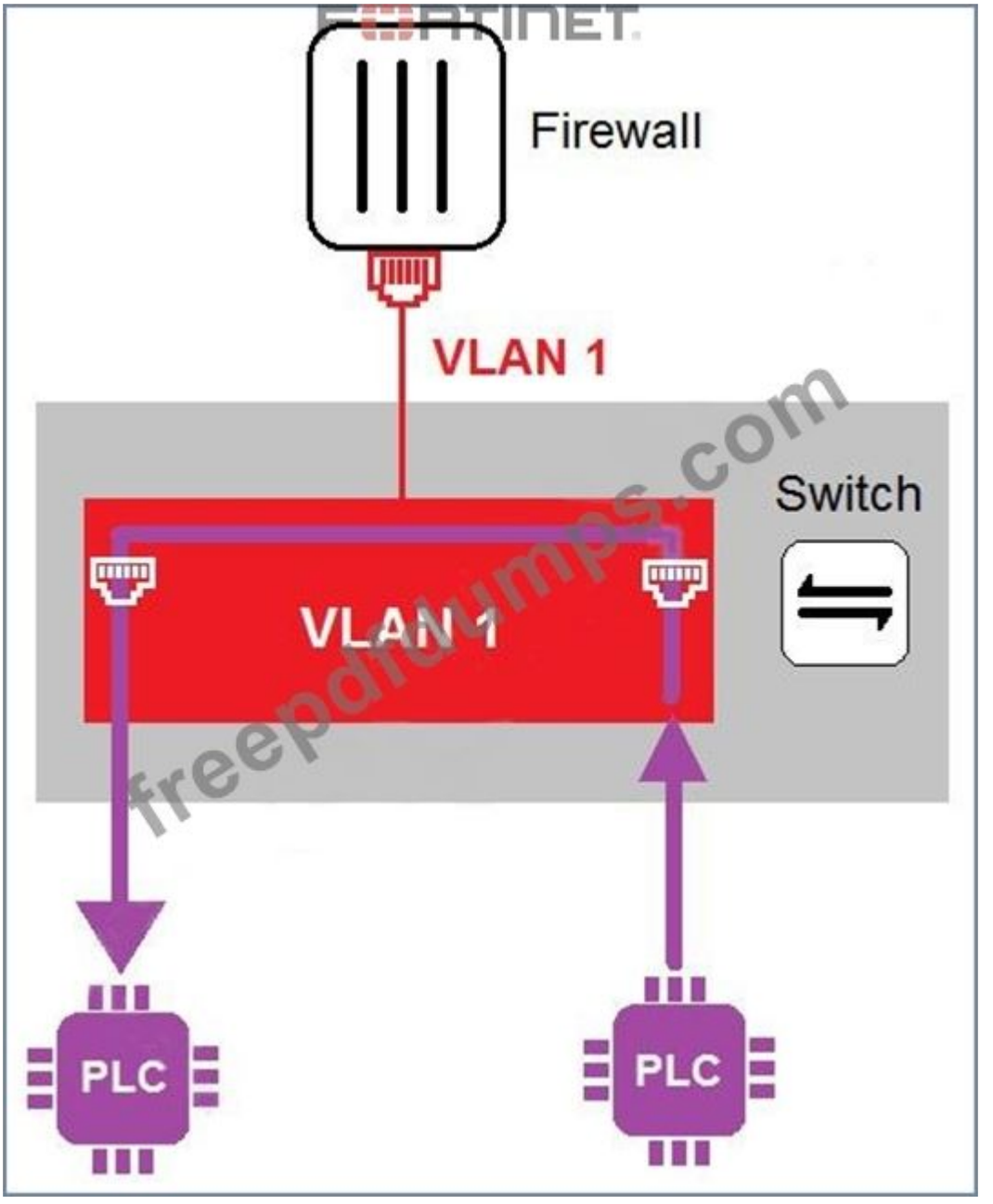
Refer to the exhibit.

An operational technology rule is created and successfully activated to monitor the Modbus protocol on FortiSIEM. However, the rule does not trigger incidents despite Modbus traffic and application logs being received correctly by FortiSIEM.
Which statement correctly describes the issue on the rule configuration?
A. The first condition on the SubPattern filter must use the OR logical operator.
B. The Aggregate attribute COUNT expression is incompatible with the filters.
C. The SubPattern is missing the filter to match the Modbus protocol.
D. The attributes in the Group By section must match the ones in Fitters section.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 13
How can you achieve remote access and internel availability in an OT network?
A. Add additional internal firewalls to access OT devices.
B. Create more access policies to prevent unauthorized access.
C. Implement SD-WAN to manage traffic on each ISP link.
D. Create a back-end backup network as a redundancy measure.
Answer: (SHOW ANSWER)

NEW QUESTION: 14

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. There is no micro-segmentation in this topology.

B. This integration solution expands VLAN capabilities from Layer 2 to Layer 3.

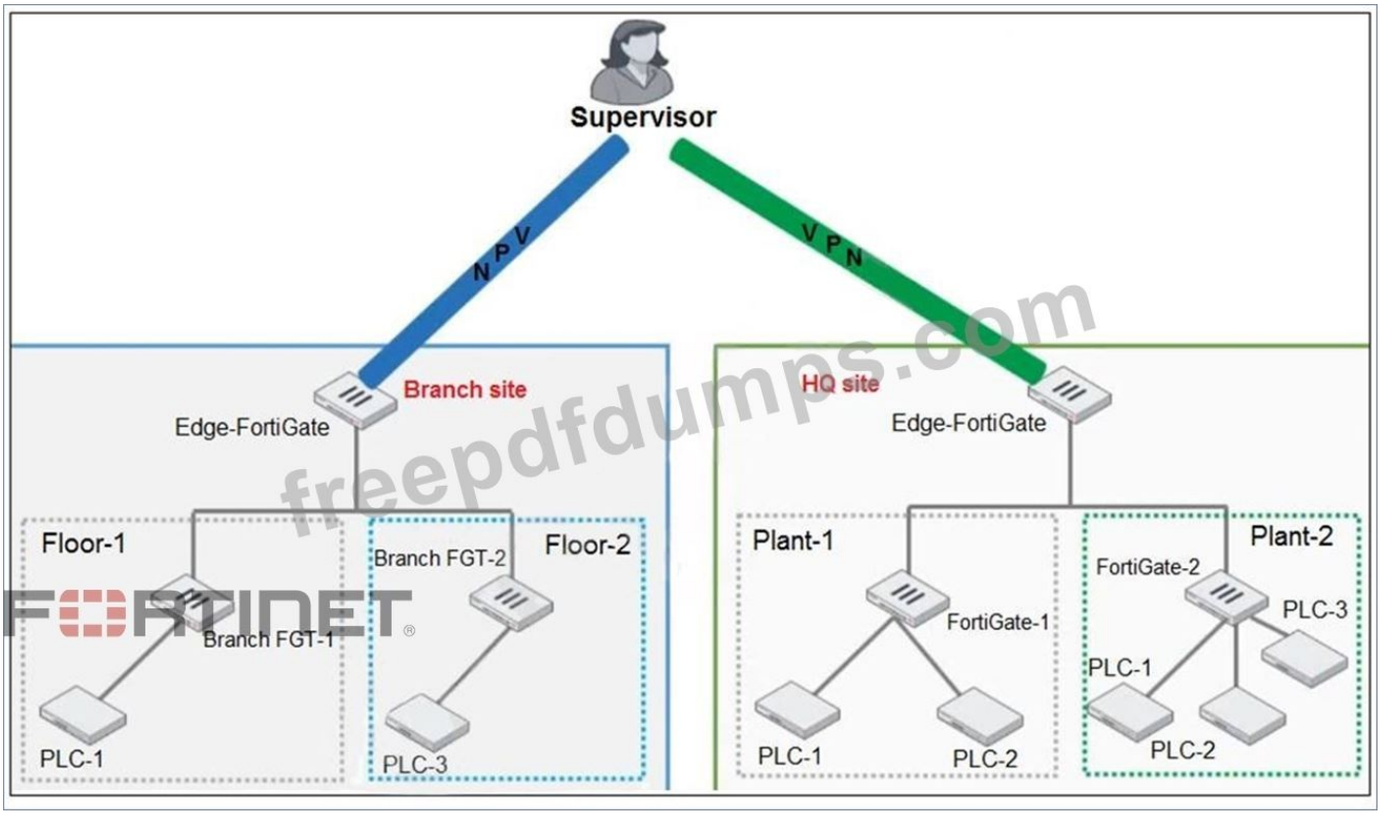
C. An administrator can create firewall policies in the switch to secure between PLCs.

D. PLCs use IEEE802.1Q protocol to communicate each other.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 15

Refer to the exhibit.



You need to configure VPN user access for supervisors at the breach and HQ sites using the same soft FortiToken. Each site has a FortiGate VPN gateway.

What must you do to achieve this objective?

A. You must use the user self-registration server.

B. You must use a FortiAuthenticator.

C. You must use a third-party RADIUS OTP server.

D. You must register the same FortiToken on more than one FortiGate.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 16

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 (LEAVE A REPLY)

NEW QUESTION: 17
Which two statements about the Modbus protocol are true? (Choose two.)
A. Modbus is used to establish communication between intelligent devices.
B. You can implement Modbus networking settings on internetworking devices.
C. Modbus uses UDP frames to transport MBAP and function codes.
D. Most of the PLC brands come with a built-in Modbus module.
Answer: B,D (LEAVE A REPLY)

NEW QUESTION: 18
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 secondary device sends data based on request from primary device.
B. It uses OSI Layer 2 and both the primary/secondary devices send data based on a matching token ring.
C. It uses OSI Layer 2 and both the primary/secondary devices always send data during the communication.
D. It uses OSI Layer 2 and the primary device sends data based on request from secondary device.
Answer: (SHOW ANSWER)

NEW QUESTION: 19
What are two critical tasks the OT network auditors must perform during OT network risk assessment and management? (Choose two.)
A. Creating disaster recovery plans to switch operations to a backup plant
B. Evaluating what can go wrong before it happens
C. Implementing strategies to automatically bring PLCs offline
D. Planning a threat hunting strategy
Answer: A,C (LEAVE A REPLY)

NEW QUESTION: 20
Which two frameworks are common to secure ICS industrial processes, including SCADA and DCS? (Choose two.)
A. Modbus
B. IEC 62443
C. NIST Cybersecurity
D. IEC104
Answer: B,D (LEAVE A REPLY)

NEW QUESTION: 21
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)

NEW QUESTION: 22
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. Risk
B. IPS
C. Security
D. List
E. Overview
Answer: (SHOW ANSWER)

NEW QUESTION: 23
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: A,D (LEAVE A REPLY)
Explanation
Typically, in a microsegmented network, NGFWs are used in conjunction with VLANs to implement security policies and to inspect and filter network communications. Fortinet FortiSwitch and FortiGate NGFW offer an integrated approach to microsegmentation.

NEW QUESTION: 24
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. FortiSandbox and FortiSIEM
B. A syslog server and FortiSIEM
C. FortiSOAR and FortiSIEM
D. FortiSIEM and FortiManager
Answer: C (LEAVE A REPLY)