Website: https://vceplus.com - https://vceplus.co - https://vceplus.io

QUESTION 1

Which three criteria can a FortiGate device use to look for a matching firewall policy to process traffic? (Choose three.)

A. Services defined in the firewall policy.

B. Source defined as internet services in the firewall policy

C. Lowest to highest policy ID number

D. Destination defined as internet services in the firewall policy

E. Highest to lowest priority defined in the firewall policy

ANSWER: A B D

QUESTION 2

An OT administrator has configured FSSO and local firewall authentication. A user who is part of a user group is not prompted from credentials during authentication.

What is a possible reason?

A. FortiGate determined the user by passive authentication

B. The user was determined by Security Fabric

C. Two-factor authentication is not configured with RADIUS authentication method

D. FortiNAC determined the user by DHCP fingerprint method

ANSWER: D

QUESTION 3

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

A. Enhanced point of connection details

B. Direct VLAN assignment

C. Adapter consolidation for multi-adapter hosts

D. Importation and classification of hosts

ANSWER: A B

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: B D

QUESTION 5

Refer to the exhibit.

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

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

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

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

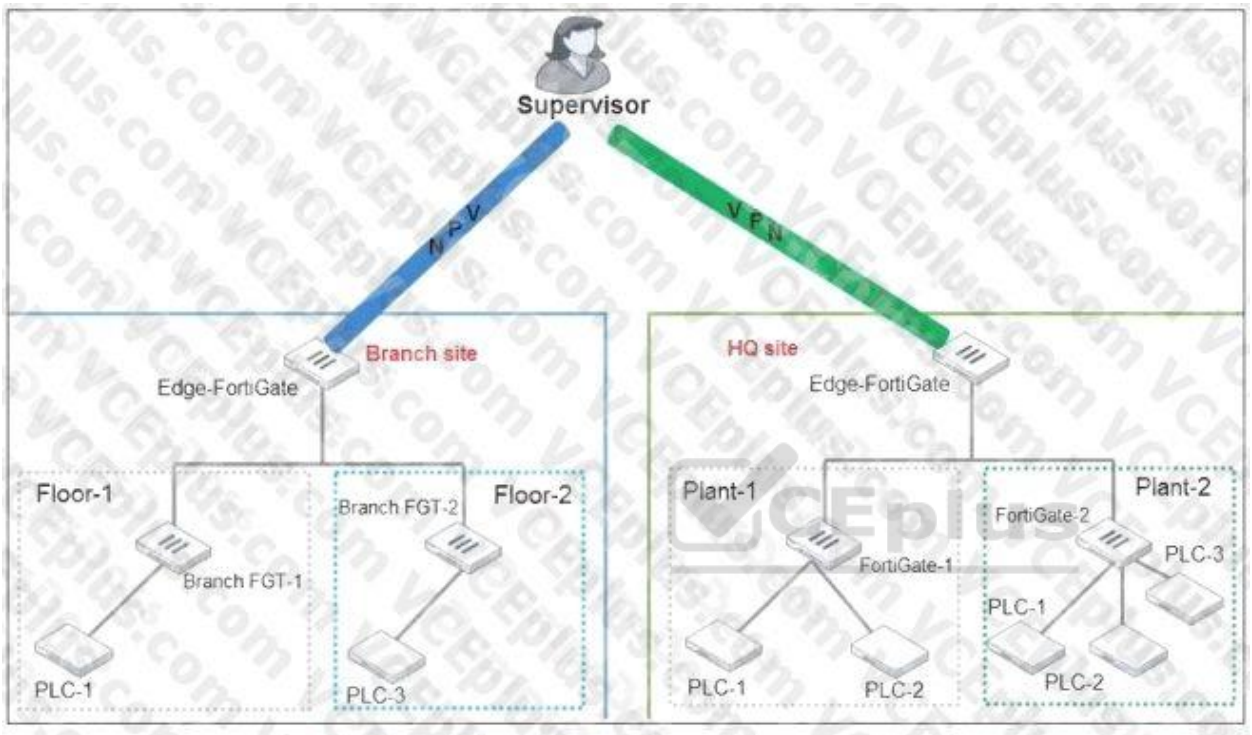
C. port1-vlan10 and port2-vlan10 are part of the same broadcast domain

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

ANSWER: D

QUESTION 6

Refer to the exhibit.



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

What must you do to achieve this objective?

A. You must use a FortiAuthenticator.

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

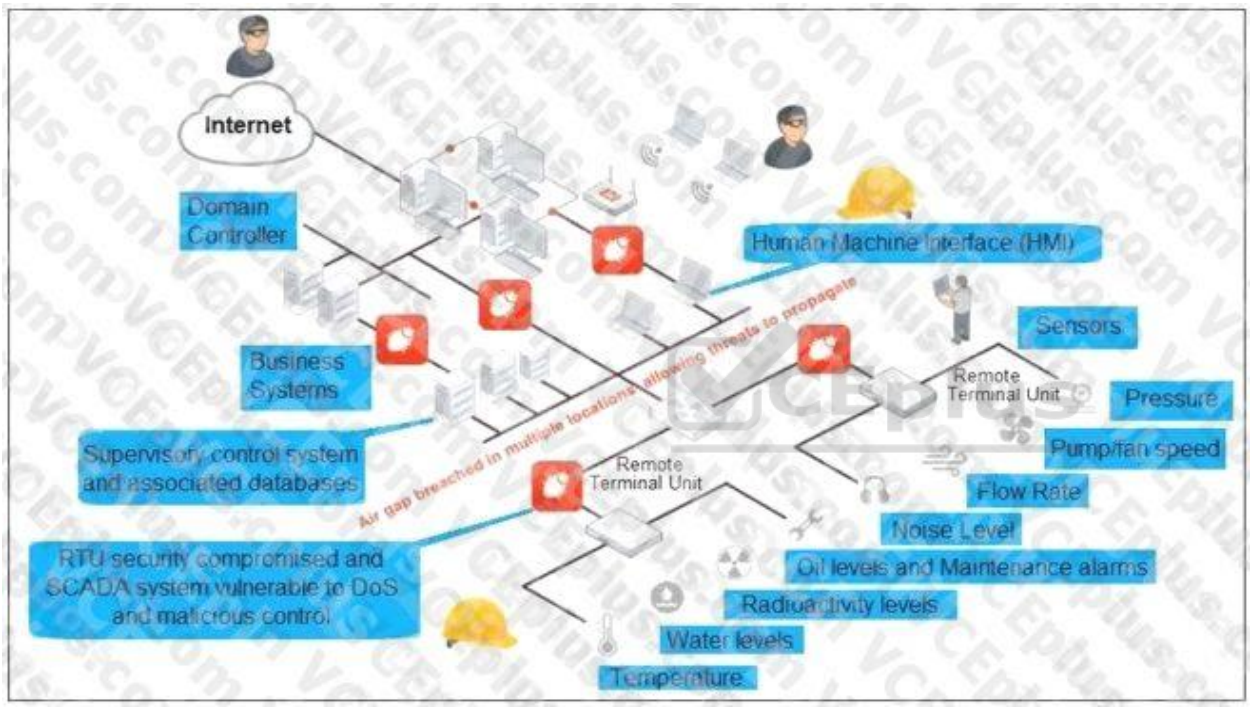
C. You must use the user self-registration server.

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

ANSWER: A

QUESTION 7

Refer to the exhibit, which shows a non-protected OT environment.



An administrator needs to implement proper protection on the OT network.

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

A. Deploy an edge FortiGate between the internet and an OT network as a one-arm sniffer.

B. Deploy a FortiGate device within each ICS network.

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

D. Configure firewall policies with industrial protocol sensors

E. Use segmentation

ANSWER: A C D

QUESTION 8

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

QUESTION 9

An OT administrator deployed many devices to secure the OT network. However, the SOC team is reporting that there are too many alerts, and that many of the alerts are false positive. The OT administrator would like to find a solution that eliminates repetitive tasks, improves efficiency, saves time, and saves resources.

Which products should the administrator deploy to address these issues and automate most of the manual tasks done by the SOC team?

A. FortiSIEM and FortiManager

B. FortiSandbox and FortiSIEM

C. FortiSOAR and FortiSIEM

D. A syslog server and FortiSIEM

ANSWER: C

QUESTION 10

Refer to the exhibit.

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

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

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

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

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

ANSWER: A

QUESTION 11

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

A. A failed Layer 3 poll

B. A matched security policy

C. A matched profiling rule

D. A linkup or linkdown trap

ANSWER: D

QUESTION 12

When you create a user or host profile, which three criteria can you use? (Choose three.)

A. Host or user group memberships

B. Administrative group membership

C. An existing access control policy

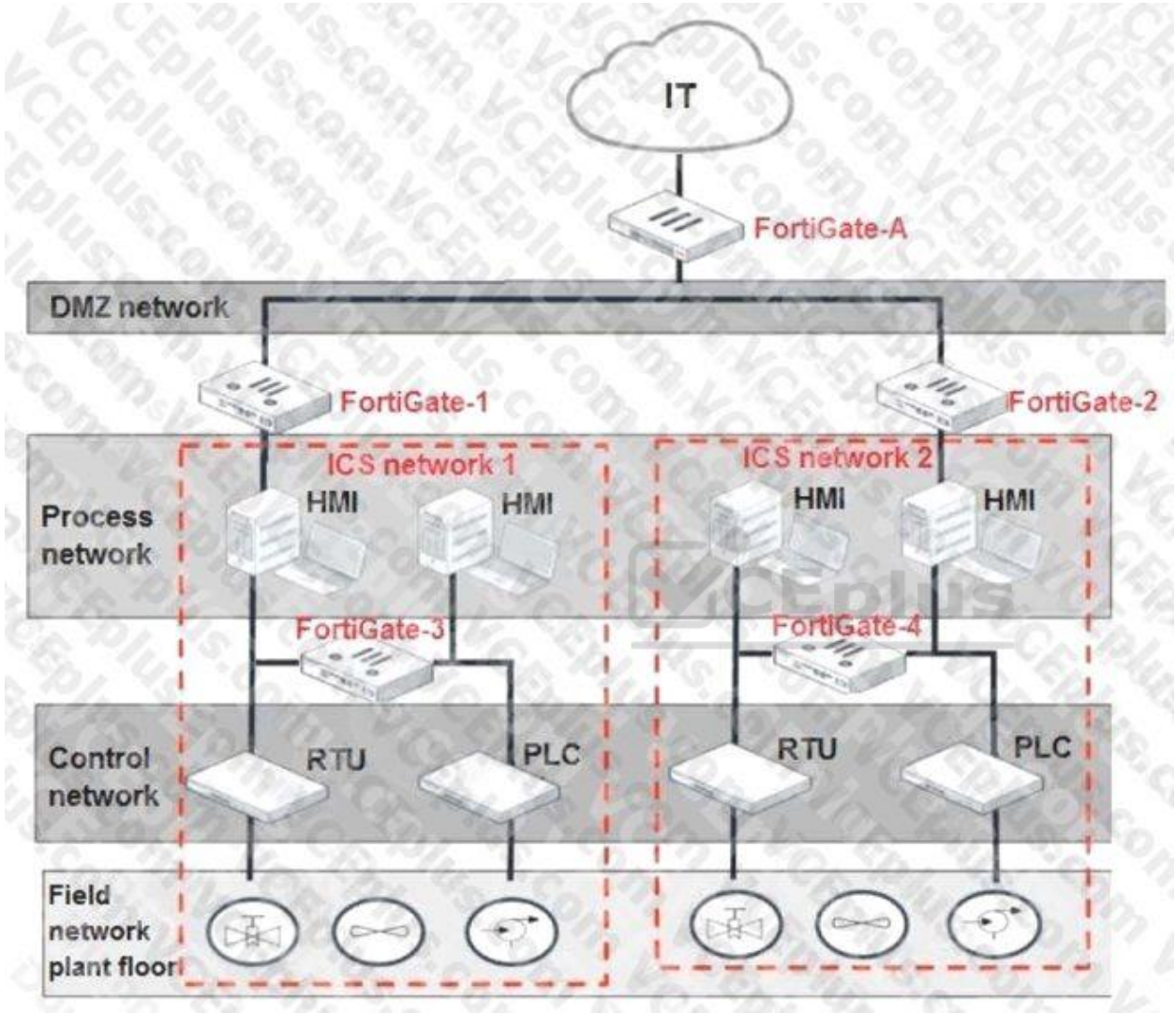
D. Location

E. Host or user attributes

ANSWER: A D E

QUESTION 13

Refer to the exhibit.



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

(Choose two.)

A. Firewall policies should be configured on FortiGate-3 and FortiGate-4 with industrial protocol sensors.

B. Micro-segmentation can be achieved only by replacing FortiGate-3 and FortiGate-4 with a pair of FortiSwitch devices.

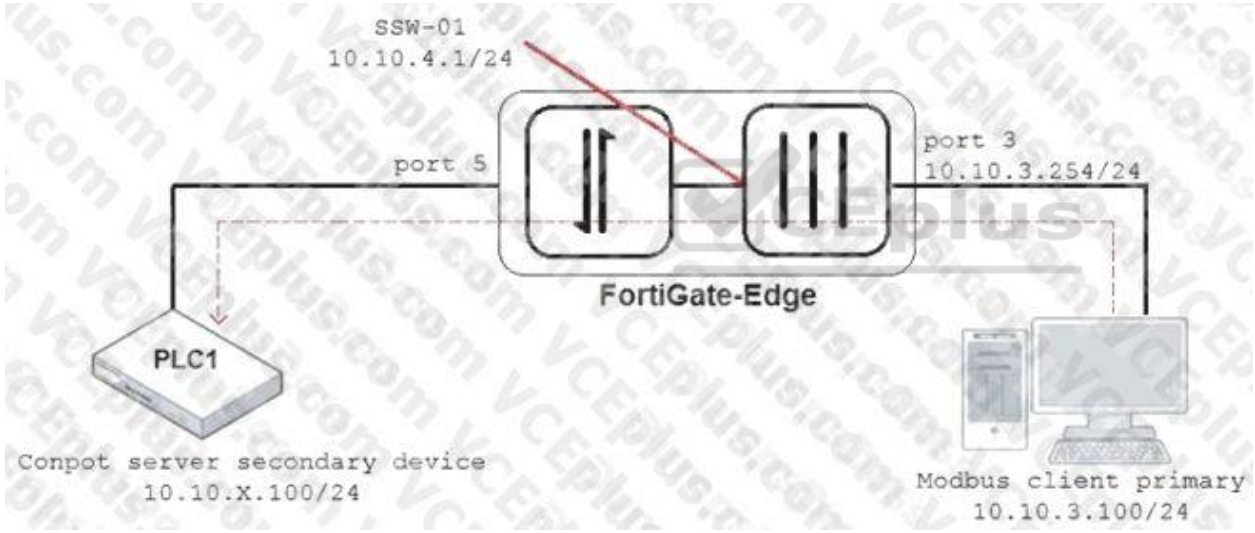
C. IT and OT networks are separated by segmentation.

D. FortiGate-3 and FortiGate-4 devices must be in a transparent mode.

ANSWER: C D

QUESTION 14

Refer to the exhibit.



An OT architect has implemented a Modbus TCP with a simulation server Conpot to identify and control the Modus traffic in the OT network. The FortiGate-Edge device is configured with a software switch interface ssw-01.

Based on the topology shown in the exhibit, which two statements about the successful simulation of traffic between client and server are true? (Choose two.)

A. The FortiGate-Edge device must be in NAT mode.

B. NAT is disabled in the FortiGate firewall policy from port3 to ssw-01.

C. The FortiGate devices is in offline IDS mode.

D. Port5 is not a member of the software switch.

ANSWER: A C

QUESTION 15

An OT supervisor has configured LDAP and FSSO for the authentication. The goal is that all the users be authenticated against passive authentication first and, if passive authentication is not successful, then users should be challenged with active authentication.

What should the OT supervisor do to achieve this on FortiGate?

A. Configure a firewall policy with LDAP users and place it on the top of list of firewall policies.

B. Enable two-factor authentication with FSSO.

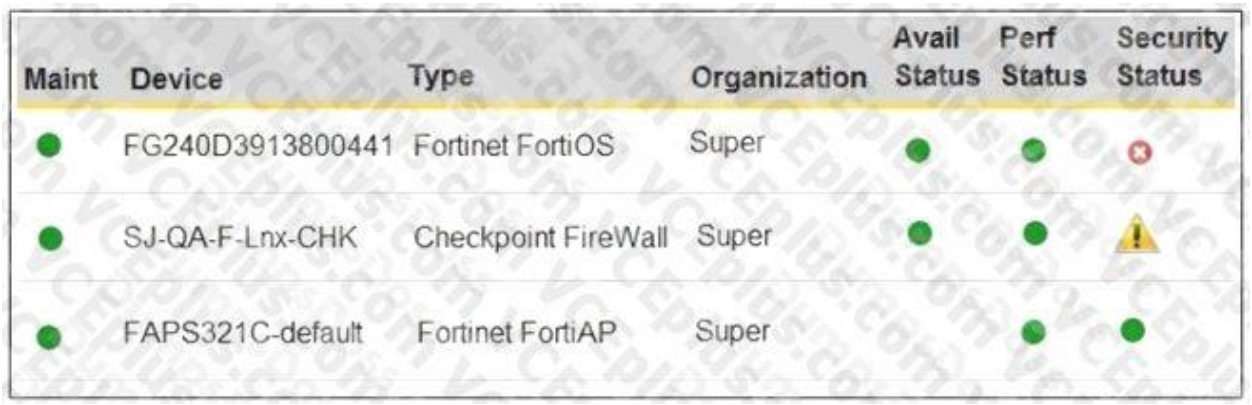
C. Configure a firewall policy with FSSO users and place it on the top of list of firewall policies.

D. Under config user settings configure set auth-on-demand implicit.

ANSWER: D

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

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: A C D

QUESTION 18

What can be assigned using network access control policies?

A. Layer 3 polling intervals

B. FortiNAC device polling methods

C. Logical networks

D. Profiling rules

ANSWER: D

QUESTION 19

An OT network architect must deploy a solution to protect fuel pumps in an industrial remote network. All the fuel pumps must be closely monitored from the corporate network for any temperature fluctuations.

How can the OT network architect achieve this goal?

A. Configure a fuel server on the remote network, and deploy a FortiSIEM with a single pattern temperature security rule on the corporate network.

B. Configure a fuel server on the corporate network, and deploy a FortiSIEM with a single pattern temperature performance rule on the remote network.

C. Configure a fuel server on the remote network, and deploy a FortiSIEM with a single pattern temperature performance rule on the corporate network.

D. Configure both fuel server and FortiSIEM with a single-pattern temperature performance rule on the corporate network.

ANSWER: B

QUESTION 20

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.

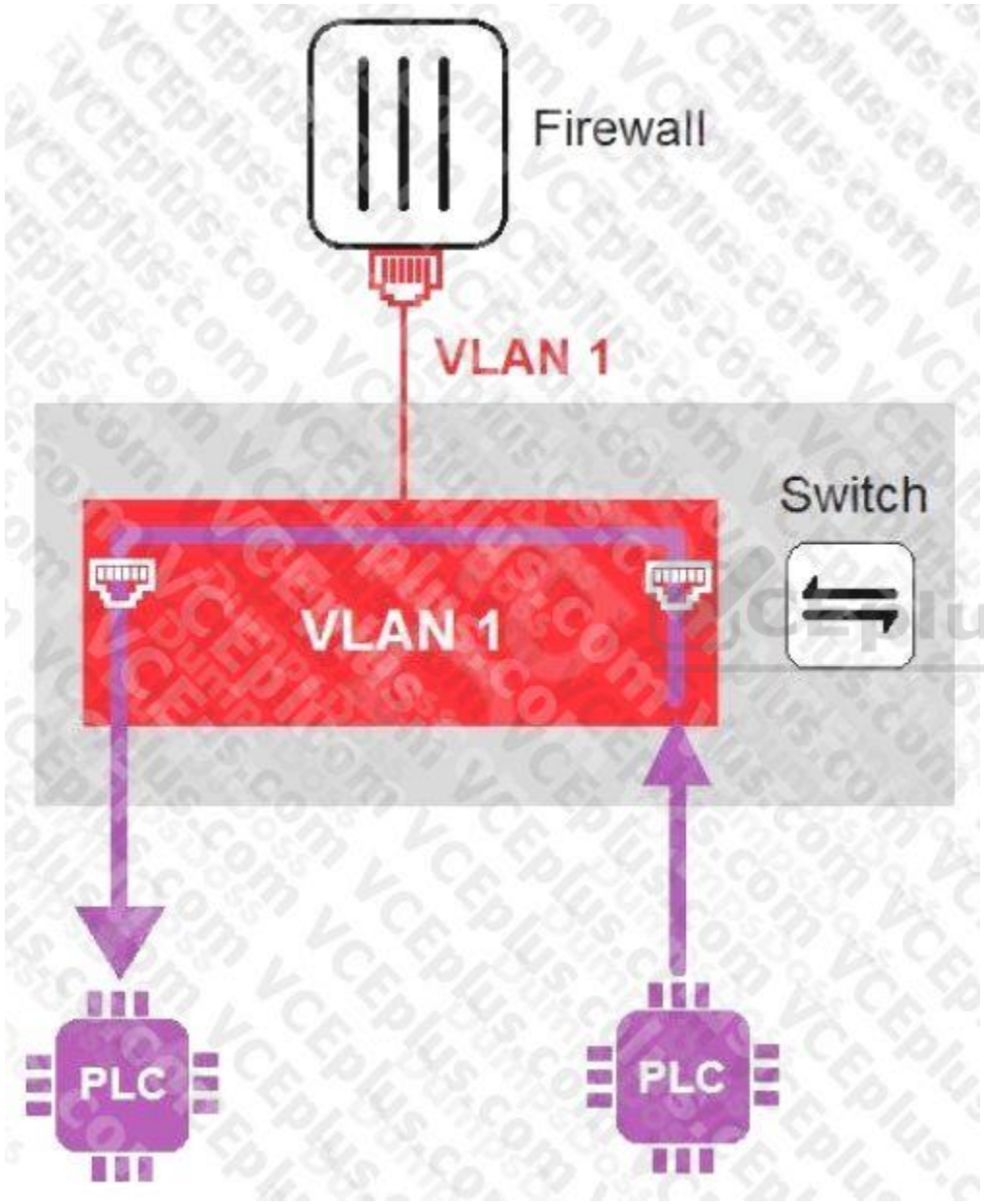
C. It can be used for network micro-segmentation.

D. It can be used for device profiling.

ANSWER: C D

QUESTION 21

Refer to the exhibit.



In the topology shown in the exhibit, both PLCs can communicate directly with each other, without going through the firewall.

Which statement about the topology is true?

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

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

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

D. There is no micro-segmentation in this topology.

ANSWER: D

QUESTION 22

Which three common breach points can be found in a typical OT environment? (Choose three.)

A. Global hat

B. Hard hat

C. VLAN exploits

D. Black hat

E. RTU exploits

ANSWER: C D E

QUESTION 23

You are investigating a series of incidents that occurred in the OT network over past 24 hours in FortiSIEM.

Which three FortiSIEM options can you use to investigate these incidents? (Choose three.)

A. Security

B. IPS

C. List

D. Risk

E. Overview

ANSWER: C D E

QUESTION 24

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

Which statement about the industrial signature database on FortiGate is true?

A. A supervisor must purchase an industrial signature database and import it to the FortiGate.

B. An administrator must create their own database using custom signatures.

C. By default, the industrial database is enabled.

D. A supervisor can enable it through the FortiGate CLI.

ANSWER: D

QUESTION 25

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

A. Known trusted devices, each time they change location

B. All connected devices, each time they connect

C. Rogue devices, only when they connect for the first time

D. Rogue devices, each time they connect

ANSWER: C

QUESTION 26

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

Which step must the administrator take to achieve this task?

A. Configure a fabric connector with a notification policy on FortiSIEM to connect with FortiGate.

B. Create a notification policy and define a script/remediation on FortiSIEM.

C. Define a script/remediation on FortiManager and enable a notification rule on FortiSIEM.

D. Deploy a mitigation script on Active Directory and create a notification policy on FortiSIEM.

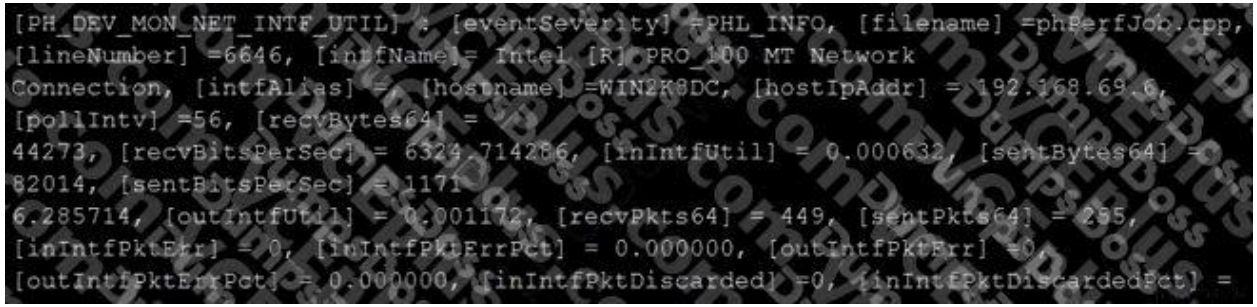
ANSWER: C

Explanation:

Reference: https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/06918379-afd1-11e9-a989-00505692583a/Standalone_PDF.pdf

QUESTION 27

Refer to the exhibit and analyze the output.



Which statement about the output is true?

A. This is a sample of a FortiAnalyzer system interface event log.

B. This is a sample of an SNMP temperature control event log.

C. This is a sample of a PAM event type.

D. This is a sample of FortiGate interface statistics.

ANSWER: A

QUESTION 28

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: D

QUESTION 29

An administrator wants to use FortiSoC and SOAR features on a FortiAnalyzer device to detect and block any unauthorized access to FortiGate devices in an OT network. Which two statements about FortiSoC and SOAR features on FortiAnalyzer are true? (Choose two.)

A. You must set correct operator in event handler to trigger an event.

B. You can automate SOC tasks through playbooks.

C. Each playbook can include multiple triggers.

D. You cannot use Windows and Linux hosts security events with FortiSoC.

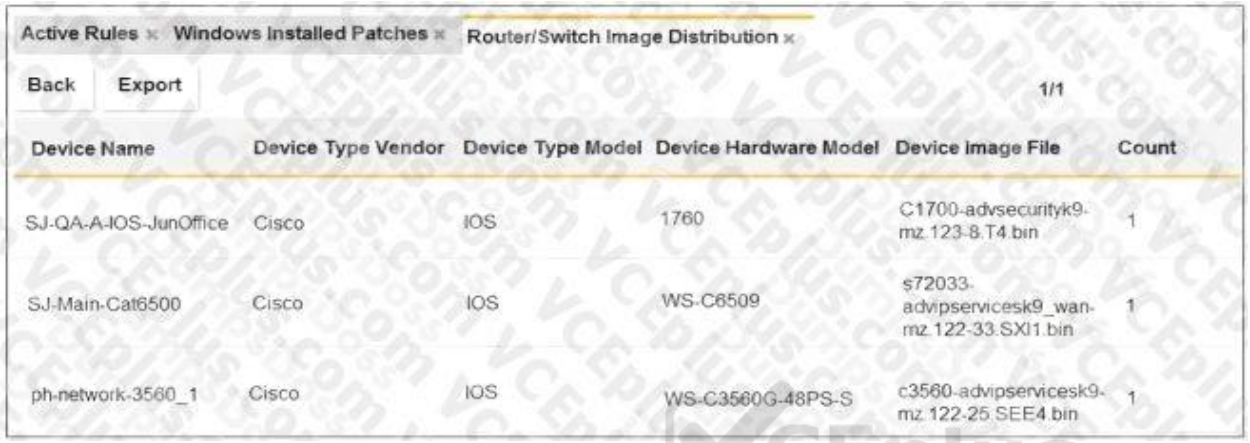
ANSWER: B C

Explanation:

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

QUESTION 30

Refer to the exhibit.



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

Back Export 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.SXI1.bin	1
ph-network-3560_1	Cisco	IOS	WS-C3560G-48PS-S	c3560-advipservicesk9-mz.122-25.SEE4.bin	1

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 FortiAnalyzer device report

C. A FortiSIEM incident report

D. A FortiSIEM analytics report

ANSWER: A

QUESTION 31

An OT architect has deployed a Layer 2 switch in the OT network at Level 1 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.

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

A. The Layer 2 switch rewrites VLAN tags before sending traffic to the FortiGate device.

B. The Layer 2 switches routes any traffic to the FortiGate device through an Ethernet link.

C. PLC1 and PLC2 traffic must flow through the Layer-2 switch trunk link to the FortiGate device.

D. In order to communicate, PLC1 must be in the same VLAN as PLC2.

ANSWER: C

QUESTION 32

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

A. SNMP

B. ICMP

C. API

D. RADIUS

E. TACACS

ANSWER: A C D

QUESTION 33

An OT network architect needs to secure control area zones with a single network access policy to provision devices to any number of different networks.

On which device can this be accomplished?

A. FortiGate

B. FortiEDR

C. FortiSwitch

D. FortiNAC

ANSWER: D

QUESTION 34

Refer to the exhibit.

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

A. FortiGate for SD-WAN

B. FortiGate for application control and IPS

C. FortiNAC for network access control

D. FortiSIEM for security incident and event management

E. FortiEDR for endpoint detection

ANSWER: B C D

QUESTION 35

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: A B