

Fortinet

Exam Questions NSE7_OTS-7.2

Fortinet NSE 7 - OT Security 7.2



NEW QUESTION 1

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

NEW QUESTION 2

Refer to the exhibit.

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.SX01.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

NEW QUESTION 3

Refer to the exhibit.

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

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

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

Answer: D

NEW QUESTION 4

How can you achieve remote access and internal availability in an OT network?

- A. Create a back-end backup network as a redundancy measure.
- B. Implement SD-WAN to manage traffic on each ISP link.
- C. Add additional internal firewalls to access OT devices.
- D. Create more access policies to prevent unauthorized access.

Answer: B

NEW QUESTION 5

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: AD

Explanation:

The two benefits of a Nozomi integration with FortiNAC are enhanced point of connection details and importation and classification of hosts. Enhanced point of connection details allows for the identification and separation of traffic from multiple points of connection, such as Wi-Fi, wired, cellular, and VPN. Importation and classification of hosts allows for the automated importing and classification of host and device information into FortiNAC. This allows for better visibility and control of the network.

NEW QUESTION 6

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: B

NEW QUESTION 7

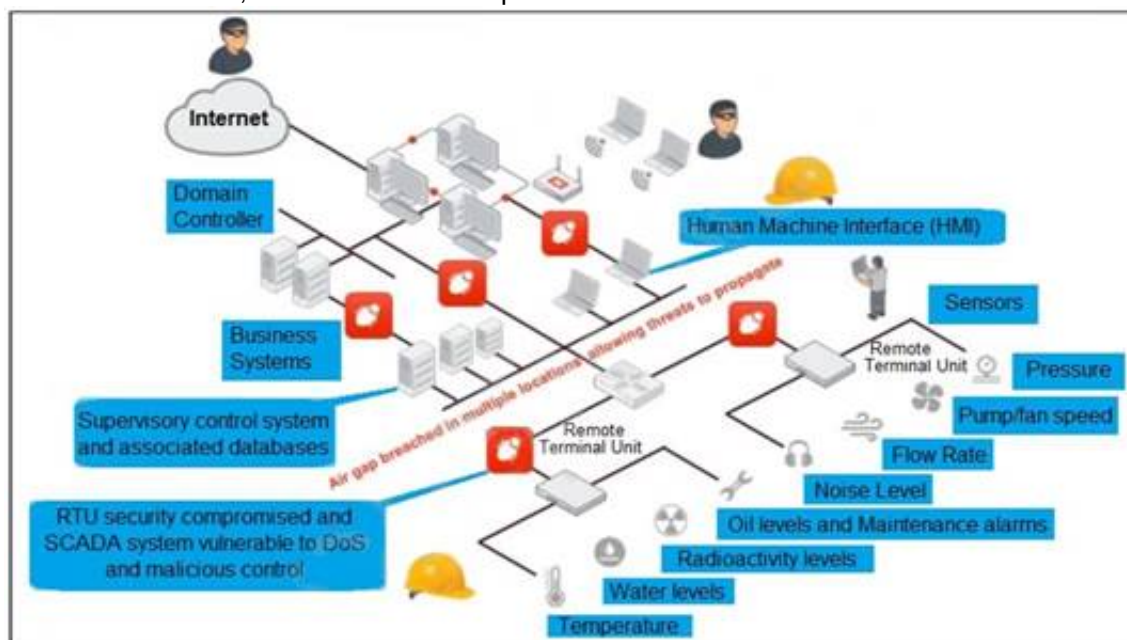
Which three methods of communication are used by FortiNAC to gather visibility information? (Choose three.)

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

Answer: ACD

NEW QUESTION 8

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: ACD

NEW QUESTION 9

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: C

Explanation:

This way, FortiSIEM can discover and monitor everything attached to the remote network and provide security visibility to the corporate network

NEW QUESTION 10

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: C

NEW QUESTION 10

An OT network consists of multiple FortiGate devices. The edge FortiGate device is deployed as the secure gateway and is only allowing remote operators to access the ICS networks on site.

Management hires a third-party company to conduct health and safety on site. The third- party company must have outbound access to external resources.

As the OT network administrator, what is the best scenario to provide external access to the third-party company while continuing to secure the ICS networks?

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

Answer: C

NEW QUESTION 12

Refer to the exhibit and analyze the output.

```
[PH_DEV_MON_NET_INTF_UTIL] : [eventSeverity] =PHL_INFO, [filename] =phPerfJob.cpp,
[lineNumber] =6646, [intfName]= Intel [R] PRO_100 MT Network
Connection, [intfAlias] =, [hostname] =WIN2K8DC, [hostIpAddr] = 192.168.69.6,
[pollIntv] =56, [recvBytes64] =
44273, [recvBitsPerSec] = 6324.714286, [inIntfUtil] = 0.000632, [sentBytes64] =
82014, [sentBitsPerSec] = 1171
6.285714, [outIntfUtil] = 0.001172, [recvPkts64] = 449, [sentPkts64] = 255,
[inIntfPktErr] = 0, [inIntfPktErrPct] = 0.000000, [outIntfPktErr] =0,
[outIntfPktErrPct] = 0.000000, [inIntfPktDiscarded] =0, [inIntfPktDiscardedPct] =
```

Which statement about the output is true?

- A. This is a sample of a FortiAnalyzer system interface event log.
- B. This is a sample of an SNMP temperature control event log.
- C. This is a sample of a PAM event type.
- D. This is a sample of FortiGate interface statistics.

Answer: C

NEW QUESTION 14

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

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

Answer: C

NEW QUESTION 17

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

- A. Services defined in the firewall policy.
- B. Source defined as internet services in the firewall policy
- C. Lowest to highest policy ID number
- D. Destination defined as internet services in the firewall policy
- E. Highest to lowest priority defined in the firewall policy

Answer: ADE

Explanation:

The three criteria that a FortiGate device can use to look for a matching firewall policy to process traffic are:

- * A. Services defined in the firewall policy - FortiGate devices can match firewall policies based on the services defined in the policy, such as HTTP, FTP, or DNS.
- * D. Destination defined as internet services in the firewall policy - FortiGate devices can also match firewall policies based on the destination of the traffic, including destination IP address, interface, or internet services.
- * E. Highest to lowest priority defined in the firewall policy - FortiGate devices can prioritize firewall policies based on the priority defined in the policy. The device will process traffic against the policy with the highest priority first and move down the list until it finds a matching policy.

Reference:

Fortinet NSE 7 - Enterprise Firewall 6.4 Study Guide, Chapter 4: Policy Implementation, page 4-18.

NEW QUESTION 20

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

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

Answer: ADE

Explanation:

A. FortiNAC - FortiNAC is a network access control solution that provides visibility and control over network devices. It can identify devices, enforce access policies, and automate threat response.

* D. FortiSIEM - FortiSIEM is a security information and event management solution that can collect and analyze data from multiple sources, including network devices and servers. It can help identify potential security threats, as well as monitor compliance with security policies and regulations.

* E. FortiAnalyzer - FortiAnalyzer is a central logging and reporting solution that collects and analyzes data from multiple sources, including FortiNAC and FortiSIEM. It can provide insights into network activity and help identify anomalies or security threats.

Reference:

Fortinet NSE 7 - OT Security 6.4 Study Guide, Chapter 4: OT Security Devices, page 4-20.

NEW QUESTION 22

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

- A. Host or user group memberships
- B. Administrative group membership
- C. An existing access control policy
- D. Location
- E. Host or user attributes

Answer: ADE

Explanation:

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

NEW QUESTION 25

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

Explanation:

The statement that is true about the traffic between PLC1 and PLC2 is that PLC1 and PLC2 traffic must flow through the Layer-2 switch trunk link to the FortiGate device.

NEW QUESTION 26

An administrator wants to use FortiSoC and SOAR features on a FortiAnalyzer device to detect and block any unauthorized access to FortiGate devices in an OT network.

Which two statements about FortiSoC and SOAR features on FortiAnalyzer are true? (Choose two.)

- A. You must set correct operator in event handler to trigger an event.
- B. You can automate SOC tasks through playbooks.
- C. Each playbook can include multiple triggers.
- D. You cannot use Windows and Linux hosts security events with FortiSoC.

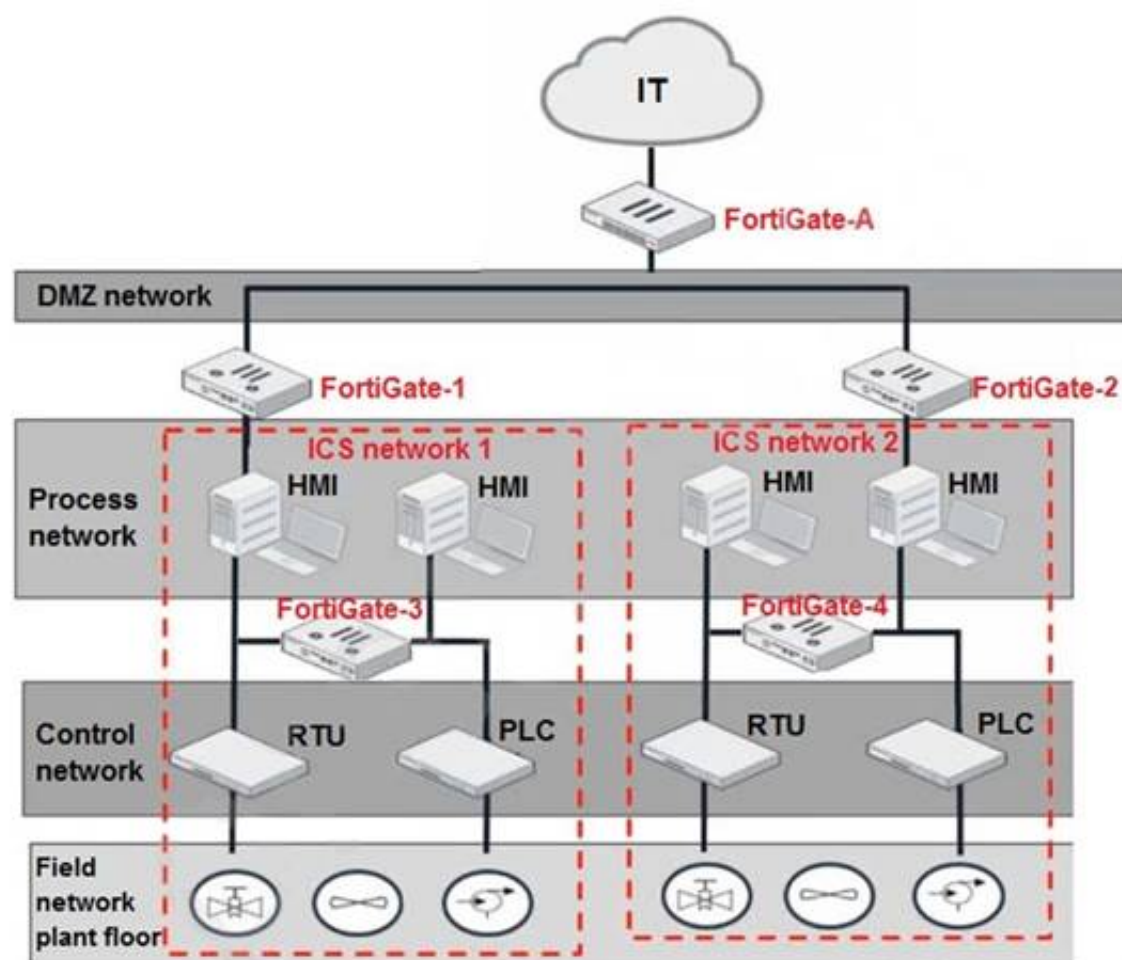
Answer: AB

Explanation:

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

NEW QUESTION 29

Refer to the exhibit.



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

- A. Firewall policies should be configured on FortiGate-3 and FortiGate-4 with industrial protocol sensors.
- B. Micro-segmentation can be achieved only by replacing FortiGate-3 and FortiGate-4 with a pair of FortiSwitch devices.
- C. IT and OT networks are separated by segmentation.
- D. FortiGate-3 and FortiGate-4 devices must be in a transparent mode.

Answer: AC

NEW QUESTION 31

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

Explanation:

FortiNAC can integrate with RADIUS servers to obtain MAC address information for wireless clients that authenticate through the RADIUS server. Reference: Fortinet NSE 7 - OT Security 6.4 Study Guide, Chapter 4: OT Security Devices, page 4-28.

NEW QUESTION 34

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

NSE7_OTS-7.2 Practice Exam Features:

- * NSE7_OTS-7.2 Questions and Answers Updated Frequently
- * NSE7_OTS-7.2 Practice Questions Verified by Expert Senior Certified Staff
- * NSE7_OTS-7.2 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * NSE7_OTS-7.2 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The NSE7_OTS-7.2 Practice Test Here](#)