

Fortinet

Exam Questions NSE7_OTS-7.2

Fortinet NSE 7 - OT Security 7.2



NEW QUESTION 1

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: BCE

NEW QUESTION 2

How can you achieve remote access and internet 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 3

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 4

Which two frameworks are common to secure ICS industrial processes, including SCADA and DCS? (Choose two.)

- A. Modbus
- B. NIST Cybersecurity
- C. IEC 62443
- D. IEC104

Answer: CD

NEW QUESTION 5

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 6

The OT network analyst runs different level of reports to quickly explore threats that exploit the network. Such reports can be run on all routers, switches, and firewalls. Which FortiSIEM reporting method helps to identify these type of exploits of image firmware files?

- A. CMDB reports
- B. Threat hunting reports
- C. Compliance reports
- D. OT/IoT reports

Answer: B

NEW QUESTION 7

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 8

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 9

Which two statements about the Modbus protocol are true? (Choose two.)

- A. Modbus uses UDP frames to transport MBAP and function codes.
- B. Most of the PLC brands come with a built-in Modbus module.
- C. You can implement Modbus networking settings on internetworking devices.
- D. Modbus is used to establish communication between intelligent devices.

Answer: BC

NEW QUESTION 10

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: AD

NEW QUESTION 10

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 11

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 12

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 14

As an OT network administrator, you are managing three FortiGate devices that each protect different levels on the Purdue model. To increase traffic visibility, you are required to implement additional security measures to detect exploits that affect PLCs.

Which security sensor must implement to detect these types of industrial exploits?

- A. Intrusion prevention system (IPS)
- B. Deep packet inspection (DPI)
- C. Antivirus inspection
- D. Application control

Answer: B

NEW QUESTION 15

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

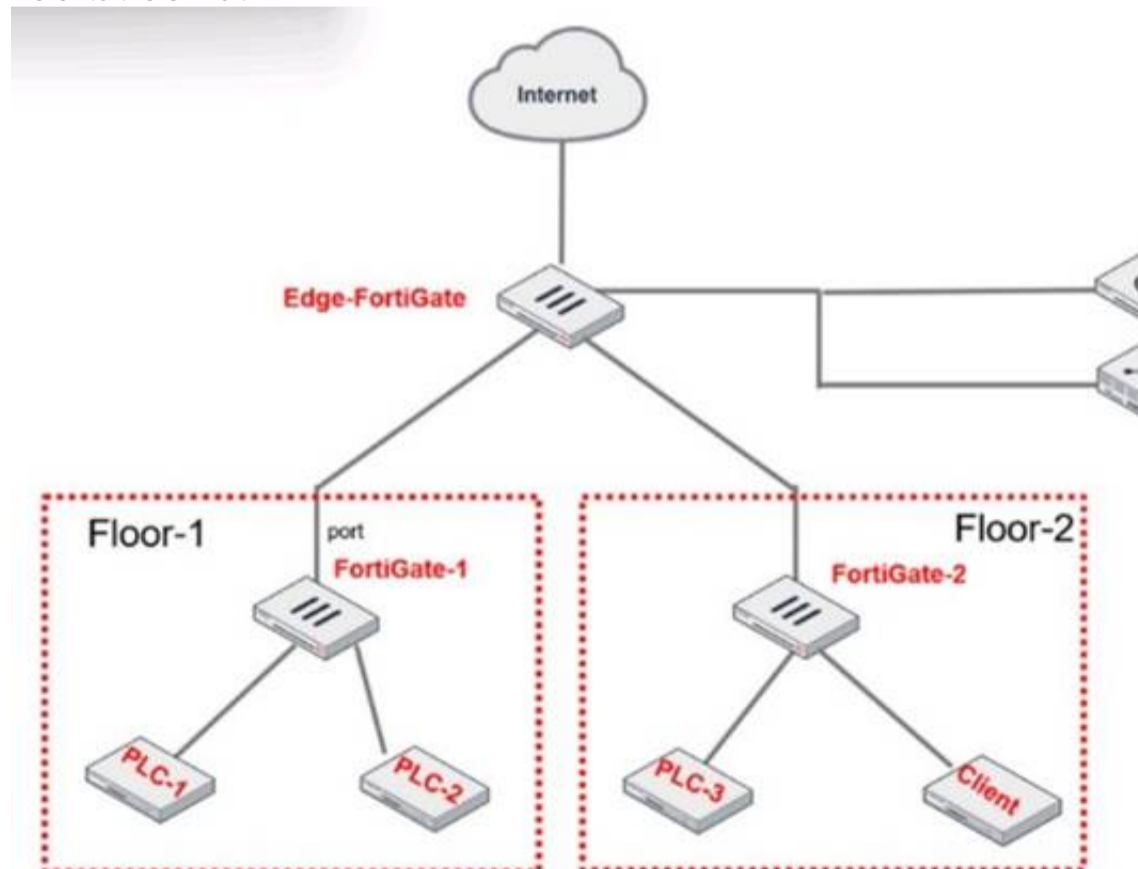
What is a possible reason?

- A. FortiGate determined the user by passive authentication
- B. The user was determined by Security Fabric
- C. Two-factor authentication is not configured with RADIUS authentication method
- D. FortiNAC determined the user by DHCP fingerprint method

Answer: A

NEW QUESTION 17

Refer to the exhibit.



PLC-3 and CLIENT can send traffic to PLC-1 and PLC-2. FGT-2 has only one software switch (SSW-1) connecting both PLC-3 and CLIENT. PLC-3 and CLIENT can send traffic to each other at the Layer 2 level.

What must the OT admin do to prevent Layer 2-level communication between PLC-3 and CLIENT?

- A. Set a unique forward domain for each interface of the software switch.
- B. Create a VLAN for each device and replace the current FGT-2 software switch members.

- C. Enable explicit intra-switch policy to require firewall policies on FGT-2.
- D. Implement policy routes on FGT-2 to control traffic between devices.

Answer: AB

NEW QUESTION 18

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 20

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 22

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 27

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: AD

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 32

Which two statements are true when you deploy FortiGate as an offline IDS? (Choose two.)

- A. FortiGate receives traffic from configured port mirroring.
- B. Network traffic goes through FortiGate.
- C. FortiGate acts as network sensor.

D. Network attacks can be detected and blocked.

Answer: BC

NEW QUESTION 34

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

NEW QUESTION 36

An OT administrator deployed many devices to secure the OT network. However, the SOC team is reporting that there are too many alerts, and that many of the alerts are false positive. The OT administrator would like to find a solution that eliminates repetitive tasks, improves efficiency, saves time, and saves resources. Which products should the administrator deploy to address these issues and automate most of the manual tasks done by the SOC team?

- A. FortiSIEM and FortiManager
- B. FortiSandbox and FortiSIEM
- C. FortiSOAR and FortiSIEM
- D. A syslog server and FortiSIEM

Answer: C

NEW QUESTION 39

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 42

.....

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](#)