DUMPSBOSS.

Fortinet NSE I - OT Security 7.6 Architect

Fortinet NSEI_OTS_AR-7.6

Version Demo

Total Demo Questions: 5

Total Premium Questions: 55

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

QUESTION NO: 1

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: A D E

Explanation:

FortiAnalyzer basic event handlers evaluate incoming logs against configured criteria and can perform immediate, built-in response and notification actions when an event is triggered. **Send alert email** is directly available as an event-handler action, allowing operations or security personnel to receive timely notification of relevant OT activity. This is useful when automation still requires a human review or escalation process.

Automatically create an incident is also available directly from the event-handler workflow. Creating an incident promotes the detected activity into FortiAnalyzer incident management, where analysts can investigate, track status, document findings, and coordinate response around the event.

Automation stitch can be selected as an event-handler action to initiate automated remediation or orchestration. An automation stitch connects a trigger to one or more actions, enabling a response process to run after the event handler identifies matching log activity. This supports OT operational workflows in which predefined, controlled actions should occur consistently after a specific security condition is detected. These configurations are part of FortiAnalyzer event management and automation capabilities; see the FortiAnalyzer 7.6 Administration Guide and Fortinet's FortiAnalyzer 7.6 documentation portal.

QUESTION NO: 2

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: A

Explanation:

Fortinet Single-Sign On (FSSO) is the appropriate FortiGate configuration for passive authentication. Passive authentication identifies users without presenting a FortiGate login prompt. Instead, FortiGate receives identity information for users who have already authenticated to the organization's directory environment, typically through a Windows domain logon. This enables firewall policies to apply access controls based on authenticated user or group identity while keeping access transparent to users.

In a large OT environment, this capability helps enforce differentiated access between operational roles, engineering workstations, administrators, and other authorized personnel without requiring repeated credential entry at each protected resource. FortiGate can use the learned user-to-IP address mappings to match identity-based policies, improving visibility and control while reducing operational friction. FSSO is therefore specifically aligned with the requirement for passive

authentication, where credentials are determined automatically from an existing authentication event rather than collected interactively by the firewall.

Fortinet describes FSSO as a mechanism that transparently identifies users after they authenticate to a domain and supports user/group-based policy enforcement. See the FortiGate Administration Guide: Fortinet Single Sign-On and the FortiGate Administration Guide: Firewall authentication.

QUESTION NO: 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: D

Explanation:

Device Detection is enabled on port3. FortiGate performs device detection at the interface level. When device identification is enabled on an interface, FortiGate observes traffic entering and leaving that interface and uses the information it learns to identify connected endpoints and third-party network devices. Identified devices can then be displayed in the Security Fabric Logical Topology, improving visibility of assets that are connected beyond that FortiGate interface.

In the exhibit, the device information associated with port3 includes an “other identified device.” That topology status is evidence that FortiGate has learned a device through traffic seen on port3. Therefore, the relevant configuration conclusion is that device detection is active for port3; it is not a setting enabled on the discovered endpoint itself. This per-interface approach is particularly useful in OT environments, where administrators can selectively enable discovery on network segments that connect industrial devices, while using the Security Fabric topology to review the resulting asset visibility.

Fortinet documents interface device identification as part of FortiGate interface configuration and describes Security Fabric topology as a visibility mechanism for detected devices. See the FortiGate 7.6 Administration Guide and the FortiGate 7.6 CLI Reference.

QUESTION NO: 4

A FortiGate device receives a copy of OT traffic from a network TAP and detects a malicious Modbus request. Why can the FortiGate device not stop that request in this deployment? (Choose one answer)

A. The FortiGate device is receiving a copy of the traffic and is not in the forwarding path.

B. The Modbus protocol cannot be inspected by FortiGate.

C. A TAP deployment prevents the FortiGate device from creating logs.

D. Security profiles can be applied only to enterprise traffic.

ANSWER: A

Explanation:

The FortiGate device is receiving a copy of the traffic and is not in the forwarding path is correct. A TAP-based or mirrored-traffic deployment supports passive visibility and detection. Although the FortiGate can generate logs and alerts from the observed traffic, it cannot prevent packets that are already travelling directly between the production devices.

Applying additional security profiles can improve inspection and detection coverage but does not make an out-of-band sensor capable of blocking production packets. Prevention requires an inline enforcement point or another integrated response mechanism that can affect the original communication path.

QUESTION NO: 5

Refer to the exhibit.

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: A C

Explanation:

OT signatures are enabled. The Application Sensor includes the Operational Technology application category. When this sensor is applied to a firewall policy, FortiGate uses the application-control signatures associated with the selected category to identify OT application traffic and protocol behavior. Application control is not limited to ports; it can inspect recognized applications and protocol signatures, providing the policy with OT-aware traffic identification.

Modbus write commands are blocked. The sensor has a specific override that allows *Modbus_Read.Holding.Registers*, while the broader *Modbus* application is assigned a block action. FortiGate application control supports granular OT and industrial-protocol signatures, including signatures that identify message-level functions. The explicit allow action permits the identified Modbus holding-register read operation, and the broader Modbus block action applies to other Modbus traffic not

matched by that more-specific exception, including Modbus write operations. This configuration implements a common OT control objective: permit a required read-only command while preventing changes to process values or device state through write commands.

Fortinet documents application-control configuration and signature-based enforcement in the FortiGate Administration Guide: Application control. Fortinet's FortiGate 7.6 documentation portal provides the associated administration and OT-security documentation.