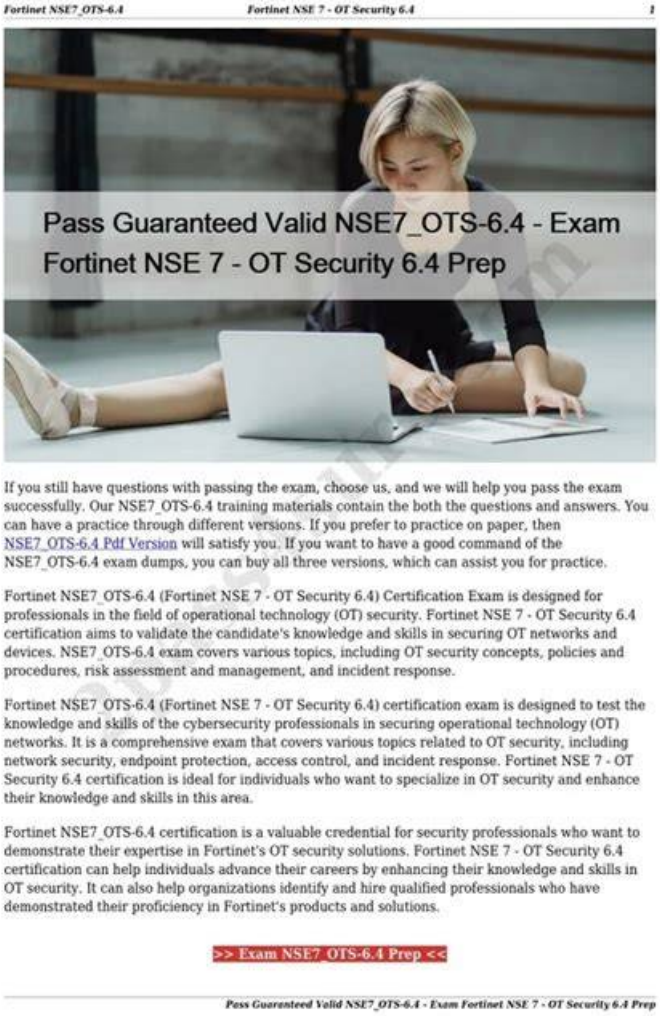
NSEI_OTS_AR-7.6 Pass Guaranteed - New Study NSEI_OTS_AR-7.6 Questions



May be you still strange to our NSEI_OTS_AR-7.6 dumps pdf, you can download the free demo of the dump torrent before you buy. If you have any questions to our Fortinet exam questions torrent, please feel free to contact us and we will give our support immediately. You will be allowed to updating NSEI_OTS_AR-7.6 Learning Materials one-year once you bought pdf dumps from our website.

Fortinet NSEI_OTS_AR-7.6 Exam Syllabus Topics:

Section	Objectives
Network security	- Configure automation - Configure virtual patching - Configure security inspections for industrial protocols
Monitoring and risk assessment	- Create FortiAnalyzer event handlers - Analyze security reports from FortiAnalyzer - Perform risk assessment and management
Network access control	- Explain OT Ethernet concepts - Configure network access authentication - Configure network segmentation schemas
Asset management	- Implement device detection on FortiGate and FortiNAC - Explain OT standard and Fortinet compliance - Fortinet Security Fabric for an OT network

>> NSEI_OTS_AR-7.6 Pass Guaranteed <<

New Study NSEI_OTS_AR-7.6 Questions - Reliable NSEI_OTS_AR-7.6 Braindumps Ppt

However, you should keep in mind to pass the Fortinet NSE I - OT Security 7.6 Architect (NSEI_OTS_AR-7.6) certification exam is not an easy task. It is a challenging job. If you want to pass the NSEI_OTS_AR-7.6 exam then you have to put in some extra effort, time, and investment then you will be confident to pass the Fortinet NSE I - OT Security 7.6 Architect (NSEI_OTS_AR-7.6) exam. With the complete and comprehensive Fortinet NSE I - OT Security 7.6 Architect (NSEI_OTS_AR-7.6) exam dumps preparation you can pass the Fortinet NSE I - OT Security 7.6 Architect (NSEI_OTS_AR-7.6) exam with good scores. The Exams4sures NSEI_OTS_AR-7.6 Questions can be helpful in this regard. You must try this.

Fortinet NSE I - OT Security 7.6 Architect Sample Questions (Q37-Q42):

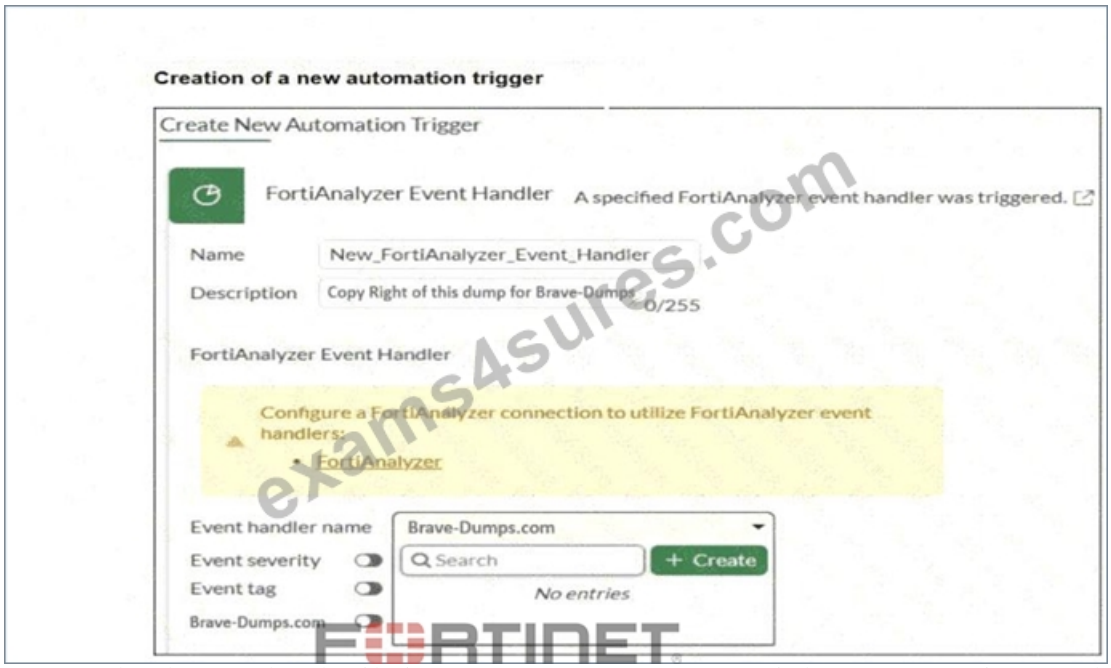
NEW QUESTION # 37
You want to improve access control for your large OT network using passive authentication. What must you configure on FortiGate? (Choose one answer)

- A. A FortiAuthenticator device as a remote server
- B. Local users
- C. Fortinet Single-Sign On (FSSO)
- D. Two-factor authentication

Answer: C

Explanation:
The correct answer is A. Fortinet Single-Sign On (FSSO) . The study guide states under Active and Passive Authentication that for passive authentication, "User does not receive a login prompt from FortiGate" ,
"Credentials are determined automatically" , and specifically "FSSO, RSSO, and NTLM can be used." It then explains that passive authentication occurs with the single sign-on method and explicitly identifies Fortinet SSO (FSSO) as one of those methods.
The guide also says: "For passive authentication, you can implement FSSO. FSSO allows users who have already authenticated on the network through another system to be transparently identified. After initial login to any system on the network, users can access allowed resources without being prompted for credentials." That is exactly what the question asks for: improving access control in a large OT network using passive authentication .
The other options do not match passive authentication. Local users are part of local authentication, two- factor authentication adds an extra security factor but still uses active authentication, and FortiAuthenticator as a remote server supports centralized authentication for mid-to-large networks, but by itself it is not the specific passive-authentication method being asked here. The study guide is explicit that the FortiGate configuration for passive authentication is FSSO .

NEW QUESTION # 38
Refer to the exhibit.



An automation trigger creation wizard is shown. You want to automate some tasks in your OT network. In a FortiGate device, you create a new automation trigger based on a FortiAnalyzer event handler. When you want to configure the Event handler name field, the event handler created in FortiAnalyzer is not shown.
What are two reasons for this? (Choose two answers)

- A. You must add the FortiGate device to FortiAnalyzer and authorize it.
- B. You must click + Create in the Event handler name field.
- C. You must configure the Fabric settings on the FortiGate device.
- D. You must enable Automation Stitch in the event handler on FortiAnalyzer.

Answer: C,D

Explanation:
The correct answers are A and B .
Option B is correct because the study guide states that "When a handler generates an event with the automation stitch option enabled, FortiAnalyzer sends a notification" to FortiGate. If Automation Stitch is not enabled in the FortiAnalyzer event handler, that handler will not be usable for the FortiGate automation- stitch workflow. The guide also explains that the configuration of each event handler can include
"Automation stitches" and "Rules," showing that this is a required part of the FortiAnalyzer-to-FortiGate automation path.
Option A is also correct. The study guide explains the automation flow in the Security Fabric:
"FortiAnalyzer parses the logs and notifies the root FortiGate" and then "The root FortiGate triggers the action." That means FortiGate must have the FortiAnalyzer connection configured through the Security Fabric side before it can consume FortiAnalyzer event handlers. The warning in the exhibit about configuring a FortiAnalyzer connection also points directly to that requirement.
Option C is incorrect because + Create is not the reason the existing event handler is missing; it is only an interface control. Option D is not the best answer for this item because the question is about why the event handler name list on FortiGate is empty for FortiAnalyzer-triggered automation. The study guide's verified requirements for that workflow are the FortiAnalyzer-to-FortiGate Fabric connection and enabling Automation Stitch on the FortiAnalyzer event handler.

NEW QUESTION # 39
Refer to the exhibit.

A basic event handler is shown. You have enabled Automation Stitch to automate the handling of an alert.
Which two steps must you take to use this automation stitch? (Choose two answers)

- A. You must configure Rules on FortiAnalyzer.
- B. You must configure Action on FortiAnalyzer.
- C. You must configure a Playbook task on FortiAnalyzer.
- D. You must configure a FortiAnalyzer event handler trigger on FortiGate.

Answer: A,D

Explanation:
The correct answers are C and D .
Option D is correct because the study guide states that the configuration of an event handler can include "Rules" and explains that "Rules are granular conditions" and "Event handlers can have one or more rules." It further states that "FortiAnalyzer uses event handlers to filter all incoming logs" and "If logs match the conditions configured in an event handler, FortiAnalyzer generates an event." Therefore, to use the automation stitch, you must define the rules on FortiAnalyzer so the event handler can actually generate the event that starts the automation flow.
Option C is also correct. The study guide explains that "When a handler generates an event with the automation stitch option enabled, FortiAnalyzer sends a notification" to the FortiGate side, and in the attack-detection example it says "FortiAnalyzer parses the logs and notifies the root FortiGate" and then
"The root FortiGate triggers the action." It also explicitly shows "Stitches configured on root FortiGate." This means the FortiGate must have the corresponding automation trigger configured for the FortiAnalyzer event handler notification.
Option A is incorrect because the study guide does not describe configuring an Action on FortiAnalyzer as the required step for this FortiAnalyzer-to-FortiGate automation-stitch flow. Option B is also incorrect because playbooks are a different FortiAnalyzer automation mechanism; the question specifically refers to using the Automation Stitch option in the event handler.

NEW QUESTION # 40
Refer to the exhibit.

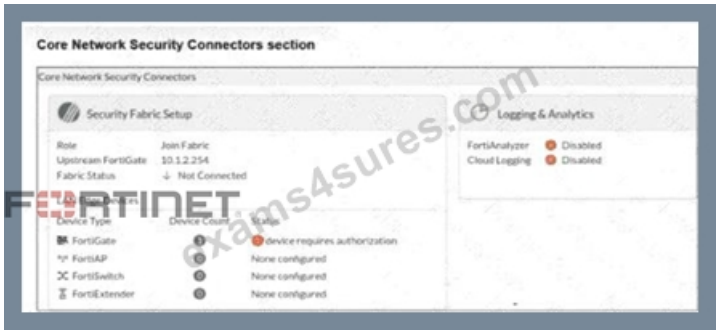
A Logical Topology page of a FortiGate device is shown. Your OT company wants to gain visibility into the network. You decide to implement device detection with the Security Fabric. Based on the exhibit, which statement is correct? (Choose one answer)

- A. Device Detection is enabled on port3.
- 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 the other identified device.

Answer: D

Explanation:
The correct answer is A. Device Detection is enabled on the other identified device .
The study guide explains that device identification is a "useful feature for the Security Fabric topology view" and that "FortiGate detects most third-party devices in your network and adds them to the topology view of the Security Fabric." It also states that in the interfaces section, you can enable device detection , and this detection is what allows FortiGate to identify devices based on observed traffic.
In the exhibit, the tooltip distinguishes between "1 device requires authorization" and "1 other identified device." That means the unauthorized device is a separate FortiGate/Fabric member issue, while the other identified device is simply a detected third-party device shown in the topology because device detection is working. Therefore, the correct interpretation is that device detection is enabled for that identified device.
Option B is incorrect because the exhibit does not say the other identified device requires authorization.
Option C is not supported by the study guide, and option D is too specific because no evidence in the exhibit confirms that the detection was enabled specifically on port3 .

NEW QUESTION # 41
Refer to the exhibit.



The Core Network Security Connectors page of the FortiGate-2 device is shown. Which statement is correct? (Choose one answer)

- A. You must configure the FortiAnalyzer settings on FortiGate-2.
- B. You must enable Security Fabric Connection on the FortiGate-2 interface.
- C. FortiGate-2 is not authorized on the root FortiGate.
- D. FortiGate-2 serves as Fabric Root.

Answer: C

Explanation:
Based on the provided exhibit and the OT Security 7.6 Architect curriculum regarding the Fortinet Security Fabric :
* Fabric Role : The exhibit clearly shows that FortiGate-2 has the role set to Join Fabric . This confirms it is a downstream device

and not the Fabric Root (eliminating Option A).
* Upstream Connection : The device is configured to point to an Upstream FortiGate at IP address 10.1.2.254 .
* Fabric Status : The status is currently displayed as Not Connected . In a standard Fortinet Security Fabric deployment, once a downstream device is configured to join the fabric, it sends a request to the upstream root device. The root FortiGate must then explicitly authorize the downstream unit before the connection is established and the status changes to " Connected. "
* Authorization Requirement : The " Not Connected " status, while having the upstream IP correctly configured, is the classic indicator that the authorization step is pending on the root FortiGate.
Furthermore, under the LAN Edge Devices section, it shows another downstream FortiGate requiring authorization on this specific unit, highlighting that authorization is a manual security requirement for all stages of the Fabric hierarchy.
* FortiAnalyzer Status : While the Logging & Analytics section shows FortiAnalyzer is Disabled , this is a configuration choice and does not prevent the Security Fabric from connecting; therefore, configuring it is not the solution to the connectivity status shown (eliminating Option C).
In summary, FortiGate-2 cannot join the fabric until an administrator logs into the Root FortiGate (10.1.2.254) and authorizes the join request from FortiGate-2.

NEW QUESTION # 42
.....

As we all know, famous companies use certificates as an important criterion for evaluating a person when recruiting. The number of certificates you have means the level of your ability. NSEI_OTS_AR-7.6 practice materials are an effective tool to help you reflect your abilities. We also hire a team of experts, and the content of NSEI_OTS_AR-7.6 question torrent is all high-quality test guidance materials that have been accepted by experienced professionals. NSEI_OTS_AR-7.6 practice materials will be the most professional and dedicated tutor you have ever met.

download □Accurate NSEI_OTS_AR-7.6 Prep Material

- myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, myportal.utt.edu.tt, scalar.usc.edu, fortunetelleroracle.com, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes