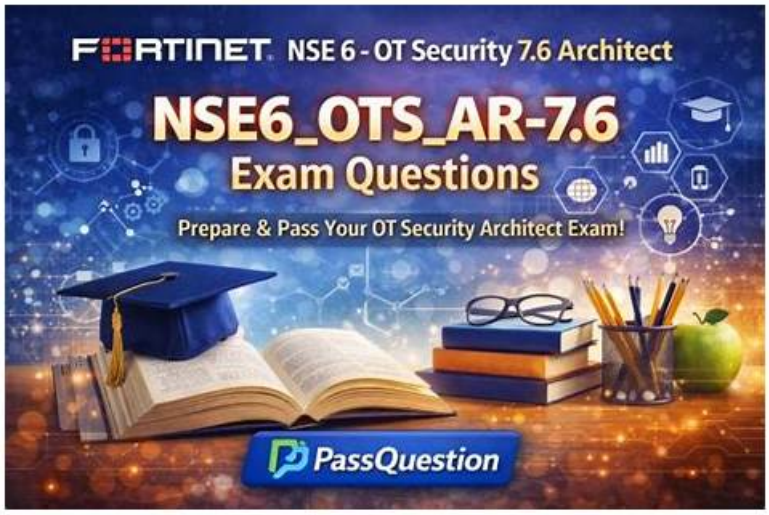
100% Pass Quiz Newest Fortinet - NSE6_OTS_AR-7.6 - Fortinet NSE 6 - OT Security 7.6 Architect Latest Test Prep



P.S. Free & New NSE6_OTS_AR-7.6 dumps are available on Google Drive shared by Dumpcollection: https://drive.google.com/open?id=1RFkbRJV4SQbLLK_o7b8rO2v9spWjBKvz

In your day-to-day life, things look like same all the time, but preparing for critical NSE6_OTS_AR-7.6 practice exam is not one of those options. About the exam ahead of you this time, our NSE6_OTS_AR-7.6 study braindumps will be your indispensable choices. Before you get the official one, you can estimate our quality by downloading the free demos. They are all masterpieces from processional experts and all content are accessible and easy to remember, so no need to spend a colossal time to practice on them. Just practice with our NSE6_OTS_AR-7.6 Exam Guide on a regular basis and desirable outcomes will be as easy as a piece of cake. On some tricky questions, you don't need to think too much. Only you memorize our questions and answers of NSE6_OTS_AR-7.6 study braindumps, you can pass exam simply.

Fortinet NSE6_OTS_AR-7.6 Exam Syllabus Topics:

Topic	Details
Topic 1	• Monitoring and risk assessment: Covers creating event handlers in FortiAnalyzer to monitor network activity and detect threats. It also includes performing risk assessments and analyzing security reports to support ongoing risk management.
Topic 2	• Asset management: Covers understanding OT standards and how Fortinet aligns with compliance requirements in industrial environments. It also includes using the Fortinet Security Fabric to manage assets and implementing device detection using FortiGate and FortiNAC.
Topic 3	• Network access control: Focuses on OT Ethernet fundamentals and designing secure network segmentation strategies. It also includes configuring authentication methods to control and verify access to the OT network.
Topic 4	• Network security: Explains how to apply security inspections specifically for industrial protocols and implement virtual patching to protect vulnerable systems. It also includes configuring automation to enhance threat response and operational efficiency.

>> NSE6_OTS_AR-7.6 Latest Test Prep <<

NSE6_OTS_AR-7.6 Actual Real Exam & NSE6_OTS_AR-7.6 Test Questions

& NSE6_OTS_AR-7.6 Dumps Torrent

The advent of our NSE6_OTS_AR-7.6 study guide with three versions has helped more than 98 percent of exam candidates get the certificate successfully. Rather than insulating from the requirements of the NSE6_OTS_AR-7.6 real exam, our NSE6_OTS_AR-7.6 practice materials closely co-related with it. And their degree of customer's satisfaction is escalating. Besides, many exam candidates are looking forward to the advent of new NSE6_OTS_AR-7.6 versions in the future.

Fortinet NSE 6 - OT Security 7.6 Architect Sample Questions (Q44-Q49):

NEW QUESTION # 44
What is the primary objective of implementing SD-WAN in operational technology (OT) networks?

- A. Replace standard links with lower cost connections
- B. Enhance network performance of OT applications
- C. Reduce security risk and threat attacks
- D. Remove centralized network security policies.

Answer: B

Explanation:
The primary objective of implementing SD-WAN in operational technology (OT) networks is to enhance the performance and reliability of OT applications. SD-WAN optimizes traffic routing based on application requirements, network conditions, and business priorities, ensuring low latency and high availability for critical OT applications. This is essential in OT environments, where the performance of applications directly impacts operational efficiency and safety.

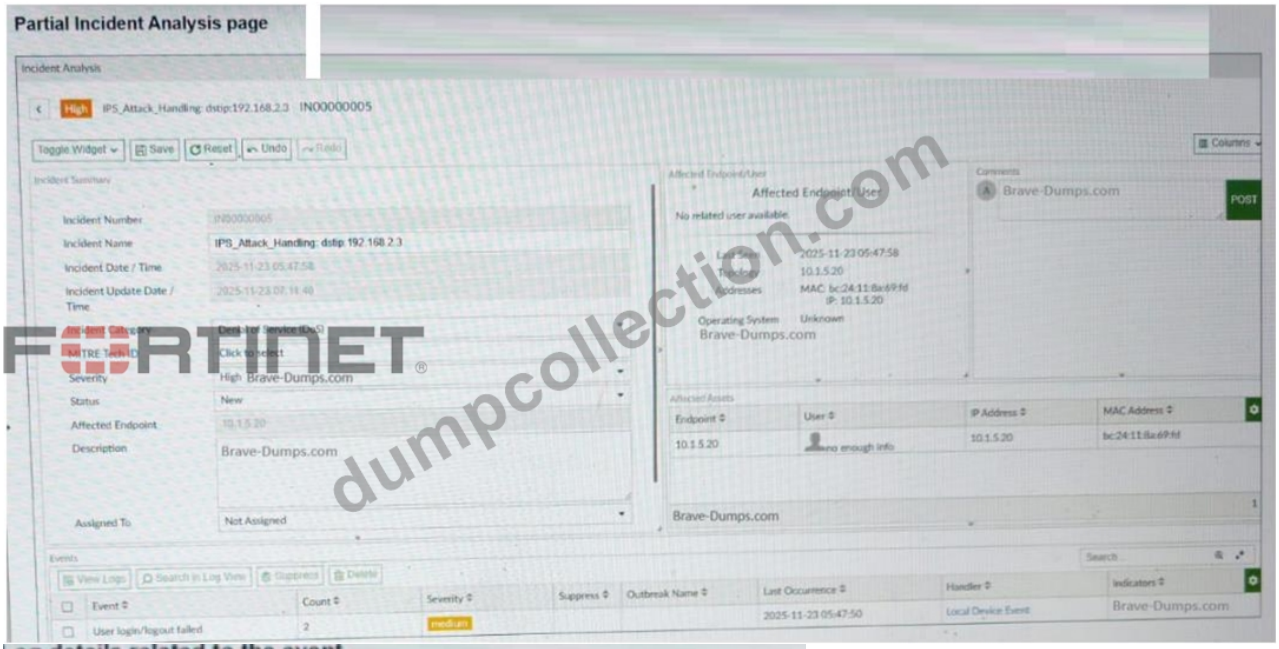
NEW QUESTION # 45
With the limit of using one firewall device, the administrator enables multi-VDOM on FortiGate to provide independent multiple security domains to each ICS network.
Which statement ensures security protection is in place for all ICS networks?

- A. Each VDOM must have an independent security license.
- B. Traffic between VDOMs must pass through the physical interfaces of FortiGate to check for security incidents.
- C. Each traffic VDOM must have a direct connection to FortiGuard services to receive the required security updates.
- D. The management VDOM must have access to all global security services.

Answer: D

Explanation:
In a multi-VDOM setup, one VDOM typically acts as the management VDOM (often called "root") which manages global settings and security services like FortiGuard updates.
This management VDOM handles access to global security services that benefit all traffic VDOMs.
Individual traffic VDOMs process their own traffic and enforce security policies but rely on the management VDOM for centralized access to global security services.
Each VDOM does not need an independent security license; the license is for the device as a whole.
Traffic between VDOMs does not need to pass through physical interfaces to be inspected; inter- VDOM links and policies handle traffic inspection.
Each VDOM does not require direct FortiGuard connections; this can be centralized in the management VDOM.

NEW QUESTION # 46
Refer to the exhibits.



A partial Incident Analysis page and the log details related to the event are shown. An attack is reported on your OT network. You analyze the corresponding incident. Based on the information provided on the Incident Analysis page and the log details, which two statements are correct? (Choose two answers)

- A. The attack uses the Modbus protocol.
- B. The target device IP address is 10.1.5.20.
- C. The event severity is high.
- D. The attack is mitigated.
- E. The attack uses the IEC 104 protocol.

Answer: A,D

Explanation:
Based on the technical data provided in the exhibits and the OT Security 7.6 Architect curriculum:
Industrial Protocol Identification (Statement A): The log details exhibit clearly shows that the Destination Port used in the attack is 502. According to the study guide's section on Industrial Protocol Protection, the standard port used by the Modbus TCP protocol is 502. Furthermore, the attack name identifies a "Triangle.Research.Nano-10.PLC," which are industrial controllers commonly

utilizing Modbus for communications.
Attack Mitigation (Statement B): The log details specify that the Action taken by the FortiGate (Edge-FortiGate) was dropped. In cybersecurity and Fortinet fabric operations, dropping a packet associated with an IPS signature means the traffic was blocked from reaching its target, thereby mitigating the attack.
Target IP Address (Statement E): The log detail explicitly lists the Destination IP as 192.168.2.3. The Incident Analysis page also titles the incident with dstip:192.168.2.3. While the "Affected Endpoint" is shown as 10.1.5.20, in an "outgoing" attack direction (as shown in the log), this likely refers to the internal source/attacker IP, whereas the target is the destination IP (192.168.2.3). Thus, Statement E is incorrect.
Protocol Conflict (Statement C): The IEC 104 protocol typically utilizes port 2404. Since the log specifies port 502, Statement C is incorrect.
Severity Distinction (Statement D): While the Incident severity is marked as High, the question specifically asks about event severity. The "Events" table at the bottom of the Incident Analysis page shows a "User login/logout failed" event with a medium severity. Because there is a distinction in the management console between the severity of individual events and the aggregated incident, and Statement A and B are technically definitive based on port and action, A and B are the correct architectural choices.

NEW QUESTION # 47
Refer to the exhibits.

A partial Basic Event Handler page on FortiAnalyzer and the creation of a trigger in a FortiGate device are shown. To improve the protection of your OT network, you want to automate the handling of compromised devices notified through FortiAnalyzer. You have configured an event handler named Alert_trigger as shown in the exhibit. When you create the trigger on the FortiGate device, the Event handler name field does not provide the Alert_trigger option. What two actions must you perform to make the Alert_trigger option available? (Choose two answers)

- A. You must authorize the FortiGate device on FortiAnalyzer.
- B. You must configure the FortiAnalyzer setting on the FortiGate device.
- C. You must click + Create in the Event handler name field.
- D. You must configure the trigger on the root FortiGate.

Answer: B,D

Explanation:
The correct answers are C and D .
Option C is correct because the study guide explains that when "a handler generates an event with the automation stitch option enabled, FortiAnalyzer sends a notification" and, in the Security Fabric workflow, "FortiAnalyzer parses the logs and notifies the root FortiGate." This means FortiGate must first have the FortiAnalyzer connection configured so it can consume FortiAnalyzer event handlers and use them in automation. The wizard message in the exhibit also points to this requirement by indicating that a FortiAnalyzer connection must be configured.
Option D is also correct because the study guide explicitly says that in this automation flow "the root FortiGate triggers the action"

and shows "Stitches configured on root FortiGate." Therefore, if you want the FortiAnalyzer event handler to appear and be usable for automation, the trigger must be configured on the root FortiGate , not on an arbitrary downstream FortiGate.
Option A is incorrect because + Create is only a GUI control and does not solve the missing-event-handler visibility problem.
Option B is not identified in the study guide as the requirement for making a FortiAnalyzer event handler available in the FortiGate automation trigger list.

NEW QUESTION # 48
What two advantages does FortiNAC provide in the OT network? (Choose two.)

- A. It can be used for device profiling.
- B. It can be used for network micro-segmentation.
- C. It can be used for IoT device detection.
- D. It can be used for industrial intrusion detection and prevention.

Answer: A,C

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 # 49
.....

- Valid NSE6_OTS_AR-7.6 Exam Camp □ Exam NSE6_OTS_AR-7.6 Duration □ NSE6_OTS_AR-7.6 Instant Discount □ Immediately open { www.vce4dumps.com } and search for 【 NSE6_OTS_AR-7.6 】 to obtain a free download □ □Exam NSE6_OTS_AR-7.6 Reference
- finnianzrta736781.blog-gold.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, tiannazmqe735216.vblogetin.com, theresailne506818.theisblog.com, agency-social.com, delilahowpm456428.bloggactivo.com, pageoftoday.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, craigcuwo886386.activoblog.com, Disposable vapes

2026 Latest Dumpcollection NSE6_OTS_AR-7.6 PDF Dumps and NSE6_OTS_AR-7.6 Exam Engine Free Share: https://drive.google.com/open?id=1RFkbRJV4SQbLLK_o7b8rO2v9spWjBKvz