Reliable Fortinet Review NSE6_OTS_AR-7.6 Guide & The Best PassTestking - Leading Provider in Qualification Exams

The PassTestking is committed to ace the NSE6_OTS_AR-7.6 exam preparation at any cost. To achieve this objective the PassTestking has hired a team of experienced and certified Fortinet NSE6_OTS_AR-7.6 exam trainers. They work together and put all their expertise to offer PassTestking NSE6_OTS_AR-7.6 Exam Questions in three different formats. These three NSE6_OTS_AR-7.6 exam practice question formats are PDF file, desktop practice test software, and web based practice test software.

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	• 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.
Topic 3	• 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 4	• 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.

>> Review NSE6_OTS_AR-7.6 Guide <<

2026 The Best 100% Free NSE6_OTS_AR-7.6 – 100% Free Review Guide | Fortinet NSE 6 - OT Security 7.6 Architect Accurate Prep Material

As long as you buy our NSE6_OTS_AR-7.6 practice materials and take it seriously to your consideration, we can promise that you will pass your NSE6_OTS_AR-7.6 exam and get your certification in a short time. We can claim that if you study with our NSE6_OTS_AR-7.6 learning guide for 20 to 30 hours as praparation, then you can be confident to pass the exam. So choose our products to help you review, you will benefit a lot from our NSE6_OTS_AR-7.6 study guide.

Fortinet NSE 6 - OT Security 7.6 Architect Sample Questions (Q109-Q114):

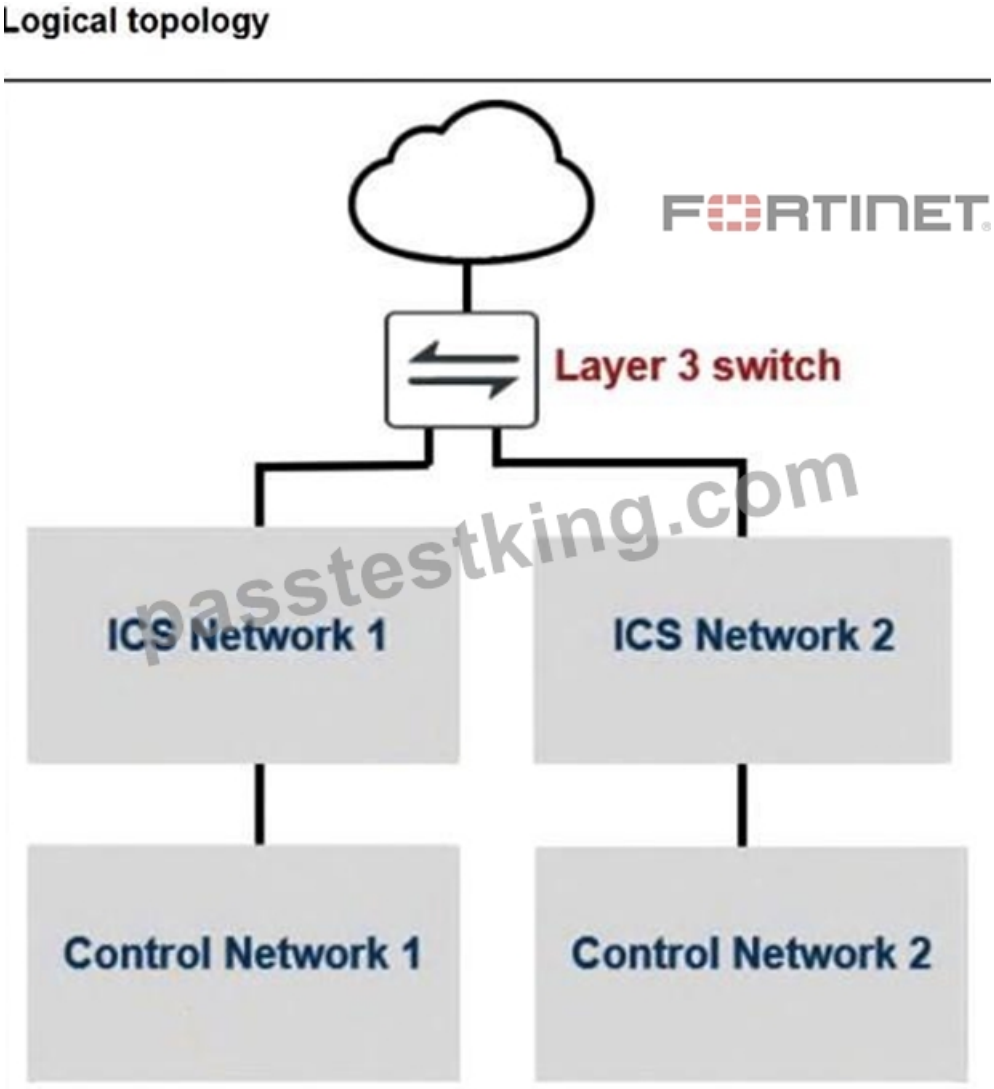
NEW QUESTION # 109
An OT administrator is defining an incident notification policy using FortiSIEM and would like to configure the system with a notification policy. If an incident occurs, the administrator would like to be able to intervene and block an IP address or disable a user in Active Directory from FortiSIEM. Which step must the administrator take to achieve this task?

- A. Configure a fabric connector with a notification policy on FortiSIEM to connect with FortiGate.
- B. Deploy a mitigation script on Active Directory and create a notification policy on FortiSIEM.
- C. Create a notification policy and define a script/remediation on FortiSIEM.
- D. Define a script/remediation on FortiManager and enable a notification rule on FortiSIEM.

Answer: C

Explanation:
https://fusecommunity.fortinet.com/blogs/silviu/2022/04/12/fortisiempublishingscript

NEW QUESTION # 110
Refer to the exhibit.



A partial OT network is shown.

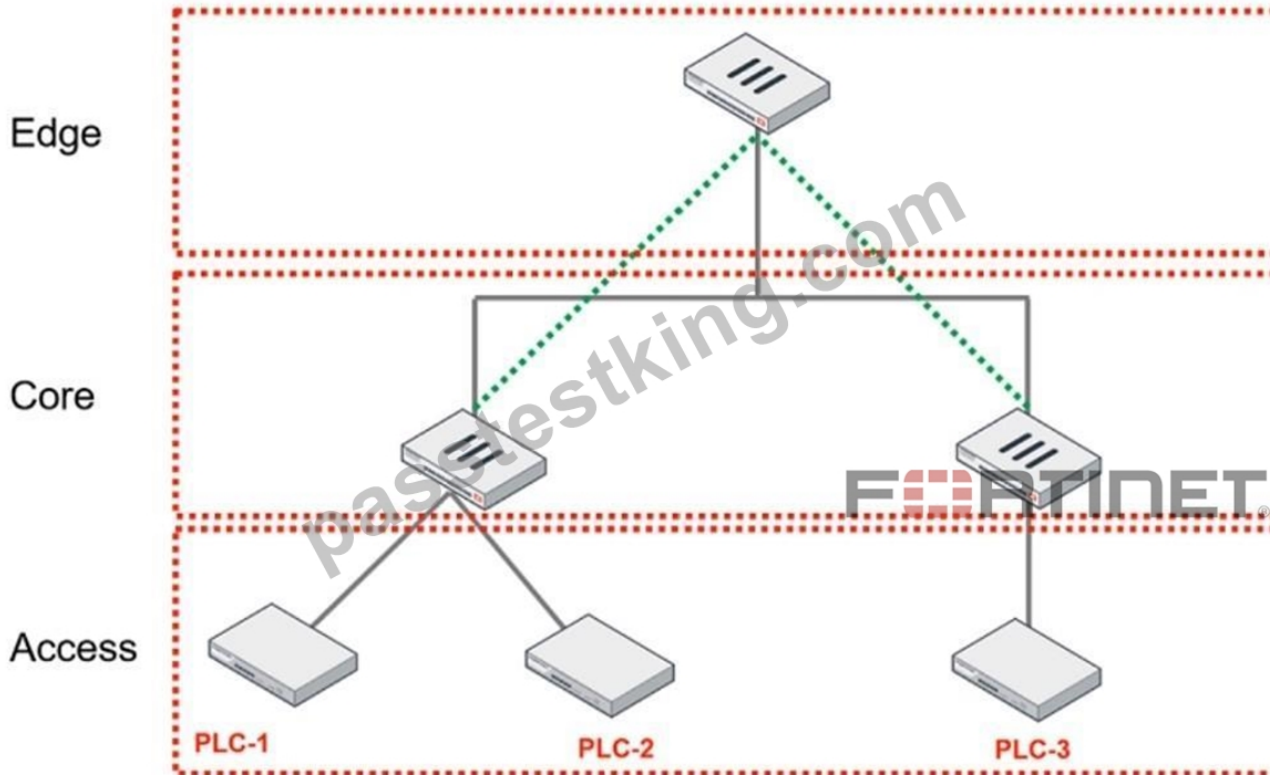
You must improve the security of this OT network and implement internal segmentation between network 1 and the network 2. How can you achieve the segmentation?

- A. You can configure one traffic VDOM.
- B. You can configure forward domain IDs for each network.
- C. You can configure universal ZTNA.
- D. You can configure an explicit software switch.

Answer: B

Explanation:
Forward domain IDs allow segmentation of traffic within the same Layer 3 infrastructure by assigning separate domains to different networks, effectively isolating Network 1 and Network 2 while still using the same physical device.

NEW QUESTION # 111
Refer to the exhibit. You are assigned to implement a remote authentication server in the OT network. Which part of the hierarchy should the authentication server be part of?



- A. Core
- B. Cloud
- C. Access
- D. Edge

Answer: D

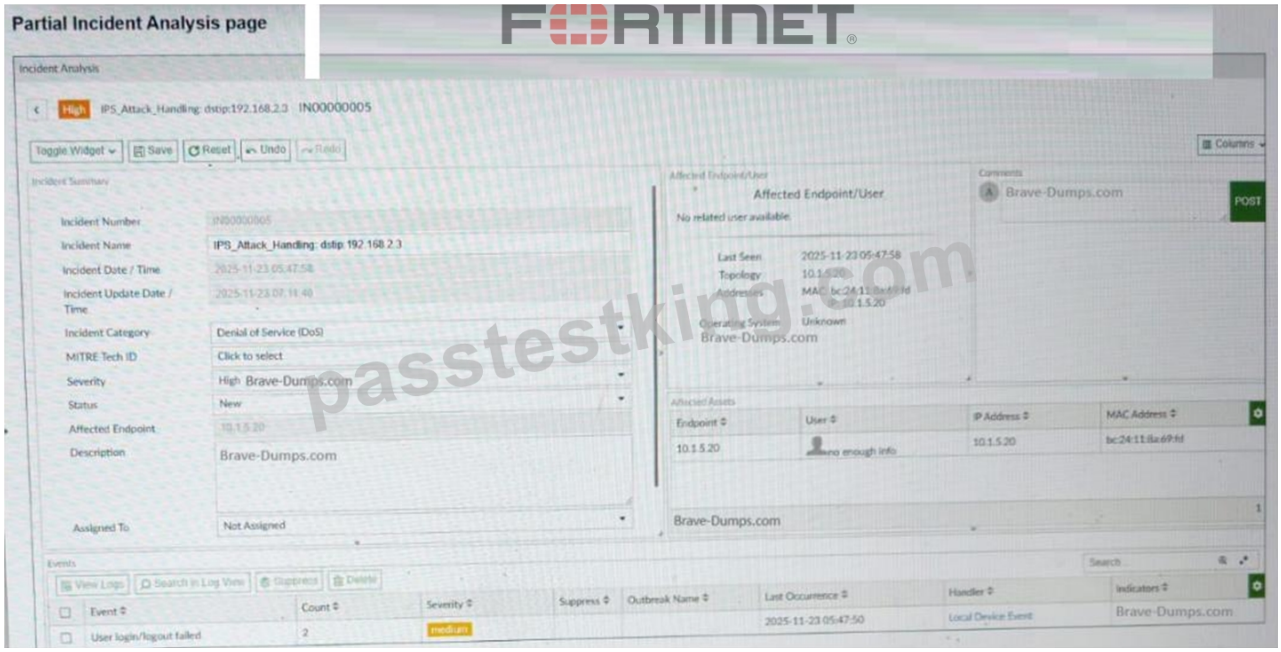
Explanation:
In a typical Purdue Enterprise Reference Architecture for OT networks, a remote authentication server for an Industrial Control System (ICS) should be located in the Edge component of the hierarchy. The Edge layer is where critical security functions are implemented to protect the lower-level control systems, making it the appropriate placement for an authentication server that validates user credentials before granting access to the OT network.

NEW QUESTION # 112
What is the main OT component for monitoring and controlling industrial processes? (Choose one answer)

- A. Industrial Control System (ICS)
- B. Supervisory Control and Data Acquisition (SCADA)
- C. Programmable Logical Controller (PLC)
- D. Industrial Internet of Things (IIoT)

Answer: A

NEW QUESTION # 113
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 target device IP address is 10.1.5.20.
- B. The event severity is high.
- C. The attack uses the Modbus protocol.
- D. The attack is mitigated.
- E. The attack uses the IEC 104 protocol.

Answer: C,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 # 114

.....

If you want to get a higher salary or a promotion on your position, you need to work harder! Purchase our NSE6_OTS_AR-7.6 learning materials and stick with it. Then your strength will protect you. For as long as you study with our NSE6_OTS_AR-7.6 exam questions, then you will find that the content of our NSE6_OTS_AR-7.6 praparation braindumps is all the hot hit of the newest knowledage and keypoints of the subject, you will learn so much to master the skills which will help you solve your problems in your work. And besides, you can achieve the certification for sure with our NSE6_OTS_AR-7.6 study guide.