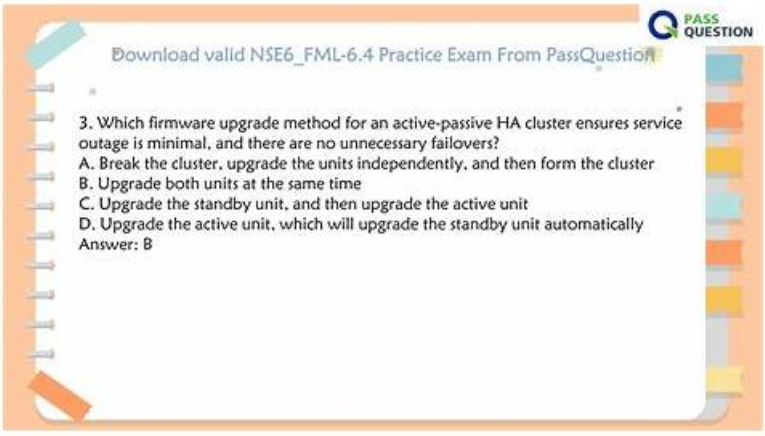
Valid NSE6_OTS_AR-7.6 Test Question - Valid Dumps NSE6_OTS_AR-7.6 Questions



About the dynamic change of our NSE6_OTS_AR-7.6 guide quiz, they will send the updates to your mailbox according to the trend of the exam. Besides, we understand you may encounter many problems such as payment or downloading NSE6_OTS_AR-7.6 practice materials and so on, contact with us, we will be there. Our employees are diligent to deal with your need and willing to do their part 24/7. They always treat customers with courtesy and respect to satisfy your need on our NSE6_OTS_AR-7.6 Exam Dumps.

Getting the Fortinet NSE 6 - OT Security 7.6 Architect (NSE6_OTS_AR-7.6) certification is the way to go if you're planning to get into Fortinet or want to start earning money quickly. Success in the Fortinet NSE 6 - OT Security 7.6 Architect (NSE6_OTS_AR-7.6) exam of this credential plays an essential role in the validation of your skills so that you can crack an interview or get a promotion in an Fortinet company. Many people are attempting the Fortinet NSE6_OTS_AR-7.6 test nowadays because its importance is growing rapidly.

>> Valid NSE6_OTS_AR-7.6 Test Question <<

Valid Dumps NSE6_OTS_AR-7.6 Questions - NSE6_OTS_AR-7.6 Downloadable PDF

Nowadays, we live so busy every day. Especially for some businessmen who want to pass the NSE6_OTS_AR-7.6 exam and get related certification, time is vital importance for them, they may don't have enough time to prepare for their exam. Some of them may give it up. After so many years' development, our NSE6_OTS_AR-7.6 exam torrent is absolutely the most excellent than other competitors, the content of it is more complete, the language of it is more simply. Believing in our NSE6_OTS_AR-7.6 Guide tests will help you get the certificate and embrace a bright future. Time and tide wait for no man. Come to buy our test engine.

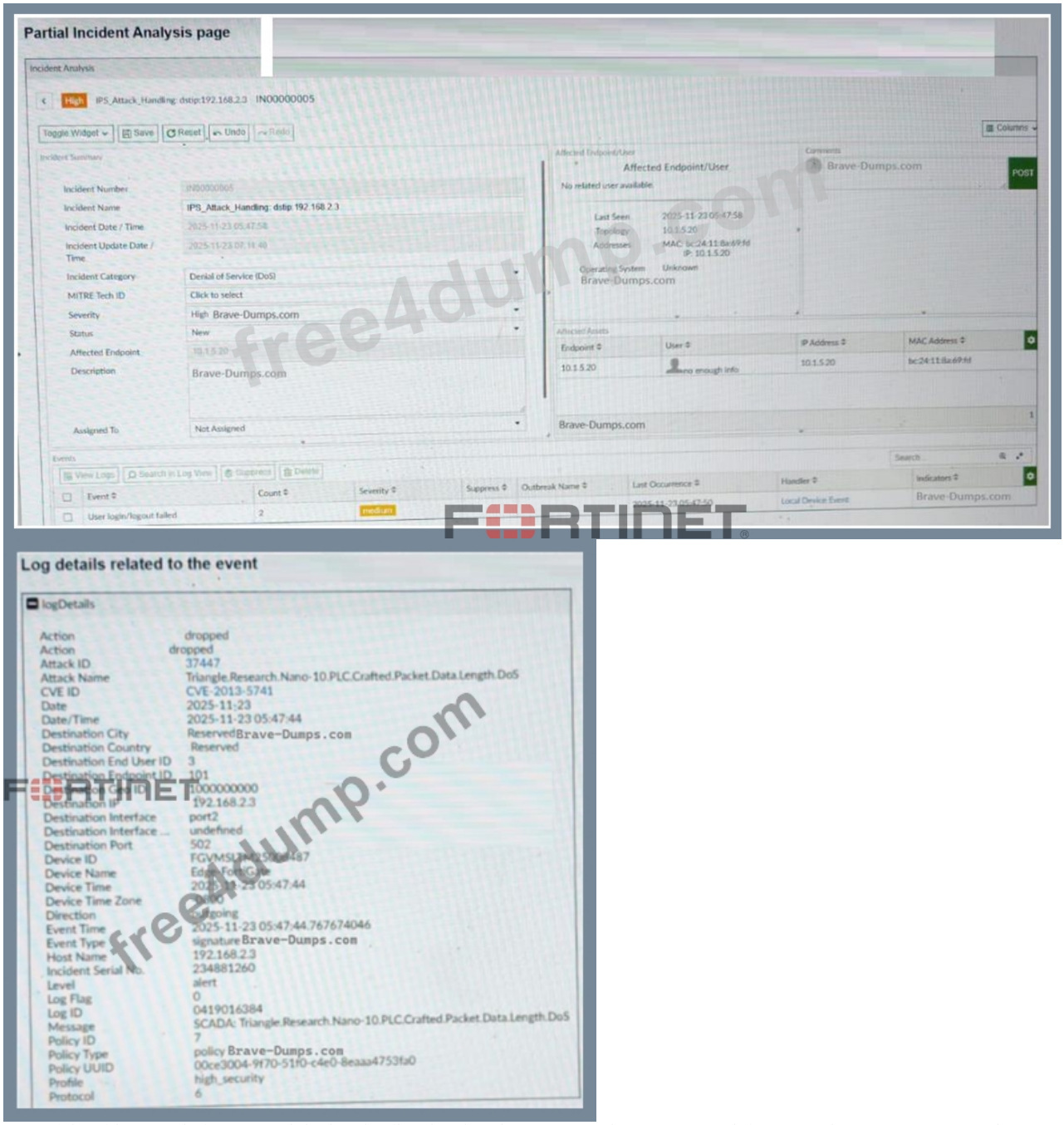
Fortinet NSE6_OTS_AR-7.6 Exam Syllabus Topics:

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 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 3	• 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 4	• 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.

Fortinet NSE 6 - OT Security 7.6 Architect Sample Questions (Q57-Q62):

NEW QUESTION # 57
Refer to the exhibits.



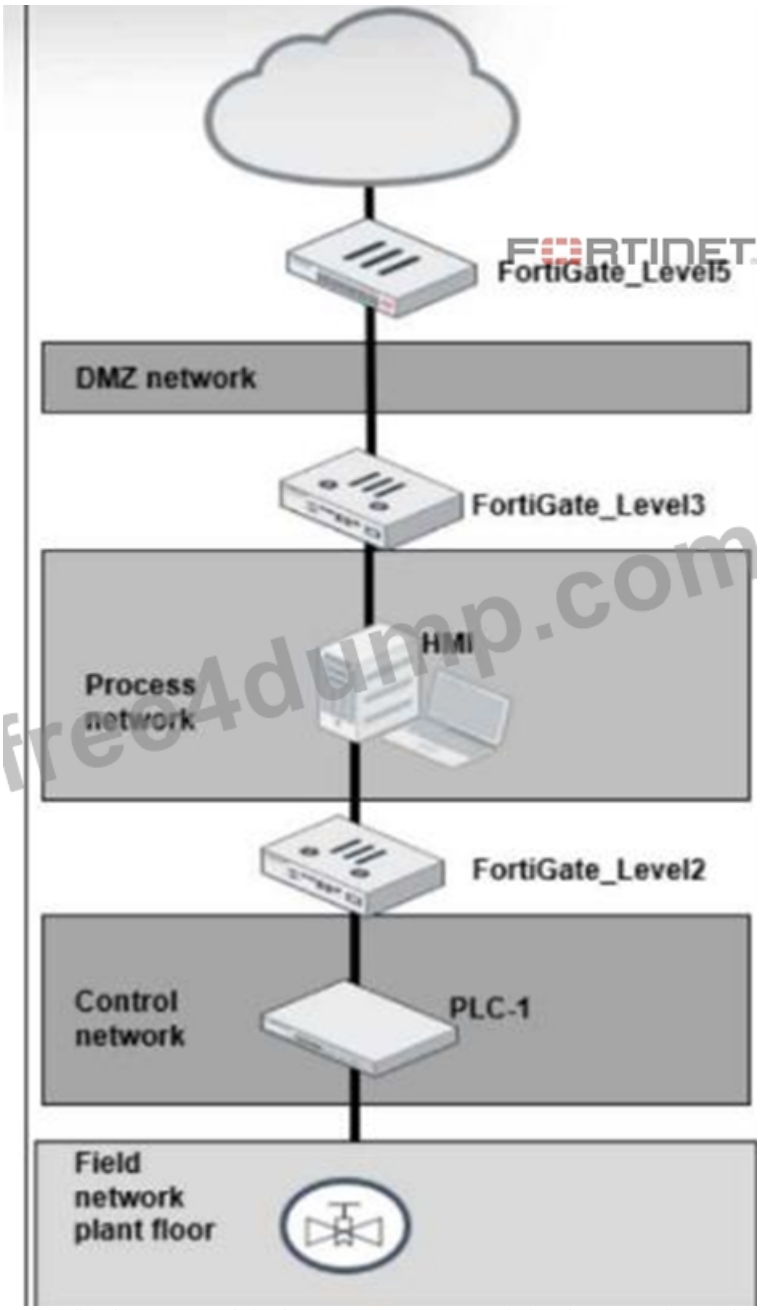
A partial Incident Analysis page and the log details related to the event are shown. An attack is reported on your OT network. You analyze the corresponding incident. Based on the information provided on the Incident Analysis page and the log details, which two statements are correct? (Choose two answers)

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

Answer: D,E

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 # 58
Refer to the exhibit.



A simplified OT network is shown. You want to optimize the protection of this OT network. Which two controls must you implement? (Choose two answers)

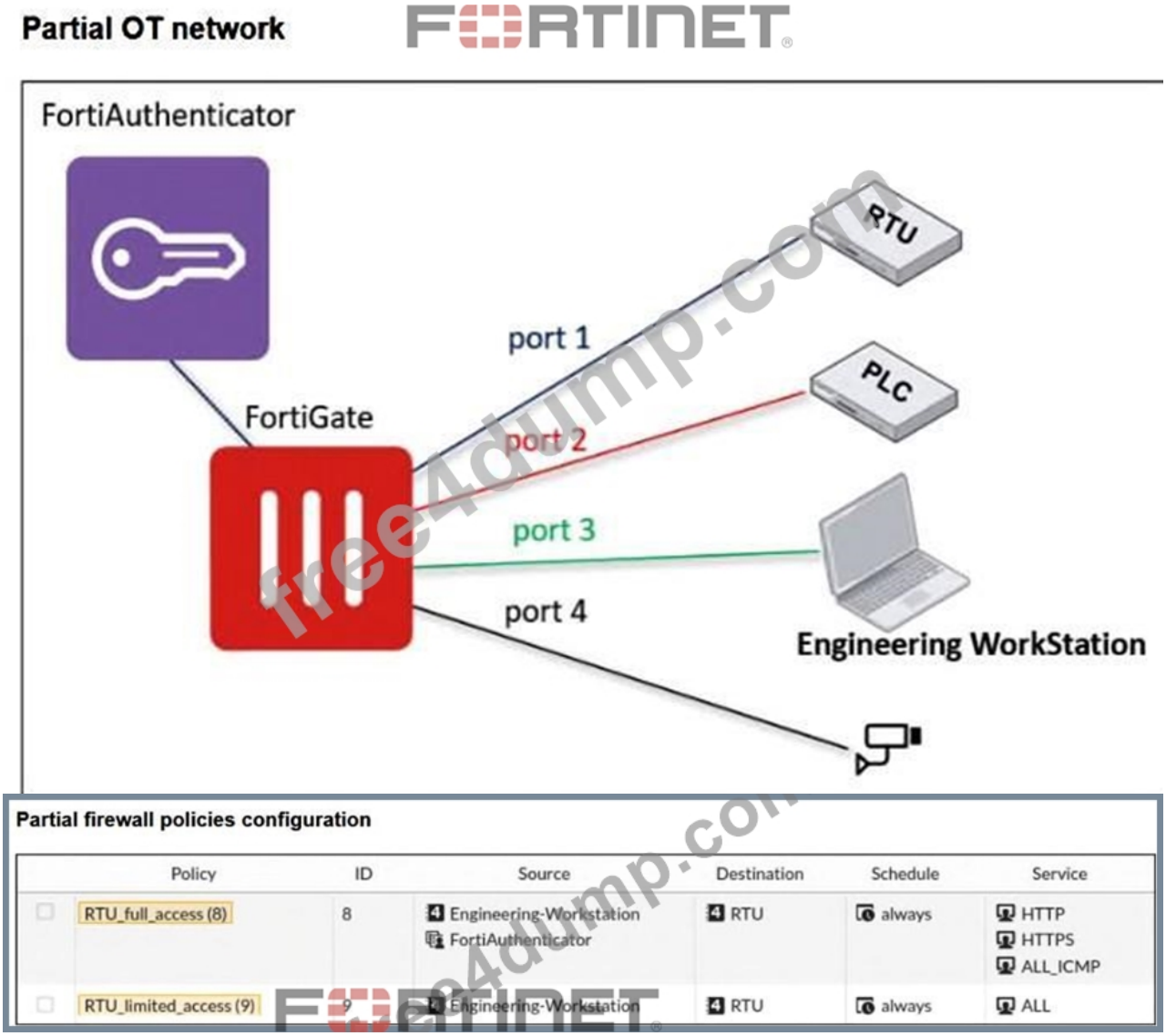
- A. OT signature on FortiGate_Level5.
- B. Virtual patching on FortiGate_Level2.
- C. Offline IDS on FortiGate_Level3.
- D. IPS on FortiGate_Level5.

Answer: B,D

Explanation:
The correct answers are B. IPS on FortiGate_Level5 and C. Virtual patching on FortiGate_Level2.
The study guide explains that "the first line of defense is securing the IT side of your network" and that FortiGate should be placed to protect ICS environments and stop threats from propagating from IT into OT. It also states that IPS improves OT security because "today's threat landscape requires IPS to block a wider range of threats and improve OT security" and that in IPS mode, vulnerable devices are protected. This makes FortiGate_Level5, at the upper boundary near the DMZ and external connectivity, the correct place to implement IPS as a primary protection control.
The study guide also states in the Purdue model section that "Level 2 consists of the processes and programs that control the PLCs, RTUs, and IEDs found at Level 1" and that "it is necessary to segment, or even microsegment, these servers with firewall segmentation, along with policies that include application control and virtual patching." In addition, the virtual patching section says "Virtual patching protects OT devices that have not yet been updated against vulnerability exploits" and applies when traffic related

to the vulnerable device reaches the firewall policy. Since FortiGate_Level2 sits between the process network and the control network, it is the right enforcement point for virtual patching to protect the PLC-side assets.
Option A is not one of the best answers because offline IDS only detects and logs attacks; the guide says "no traffic flows through FortiGate" in offline IDS mode, whereas IPS can actually block threats. Option D is also not the best answer because OT signatures are enabled within the IPS framework, but the stronger control explicitly described for this design is to deploy IPS at the upper boundary and virtual patching closer to vulnerable OT devices.

NEW QUESTION # 59
Refer to the exhibits.



Partial firewall policies configuration

Policy	ID	Source	Destination	Schedule	Service
RTU_full_access (8)	8	Engineering-Workstation FortiAuthenticator	RTU	always	HTTP HTTPS ALL_ICMP
RTU_limited_access (9)	9	Engineering-Workstation	RTU	always	ALL

A partial OT network and firewall policies configuration are shown.
You added authentication in the firewall policy from Engineering Workstation to RTU to improve the security. When verifying your configuration, you notice that you can still access RTU from Engineering Workstation without an authentication prompt.
What must you do to enforce authentication?

- A. You must add authentication in firewall policy 9.
- B. You must add a local user instead of FortiAuthenticator.
- C. You must reboot FortiGate.
- D. You must enable Fortinet Single Sign-On (FSSO).

Answer: A

Explanation:
Firewall policies are evaluated top-down, and a matching policy without authentication is applied before the one requiring authentication. Adding authentication to the higher-priority policy ensures that all matching traffic is subject to authentication.

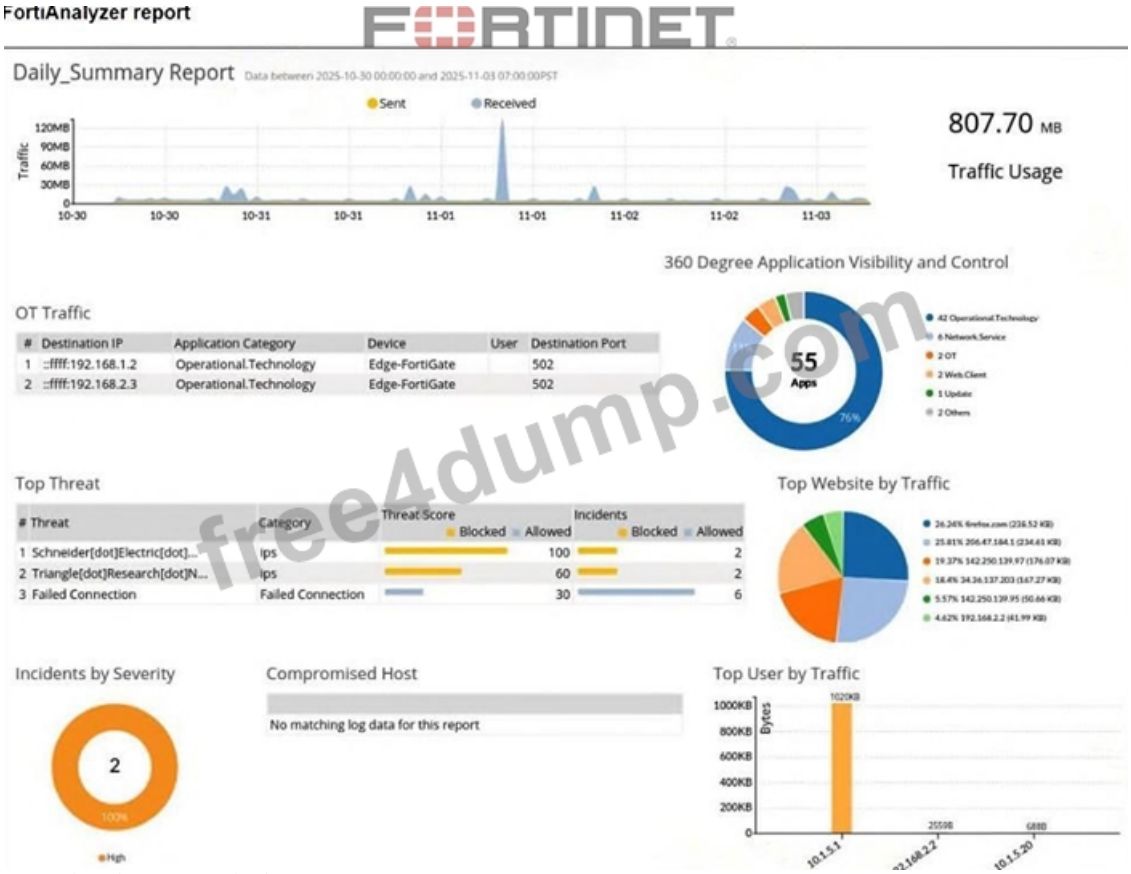
NEW QUESTION # 60
During layer 2 polling, which two pieces of information are gathered by FortiNAC to identify a device? (Choose two answers)

- A. The MAC-to-IP correlation learned
- B. The time it was learned
- C. Where it was learned
- D. The system name learned

Answer: B,C

Explanation:
According to the OT Security 7.6 Architect study guide section on Asset Management, specifically regarding FortiNAC Visibility:
Layer 2 Polling Data: Because each physical address is unique, FortiNAC identifies hosts as they connect to the network. The information gathered during this process fills in the physical address and location information in the database.
Visibility Components: The guide states that the physical address learned, the time it was learned, and where it was learned from provide the foundation of endpoint visibility in the form of "what, where, and when" information. This confirms that Where it was learned (Option A) and The time it was learned (Option D) are correct.
Exclusions:
Layer 3 Polling: The MAC-to-IP correlation (Option B) is explicitly defined as a function of Layer 3 polling, where the correlated IP address is added to the database record for the corresponding MAC address.
DHCP Fingerprinting: The host name or system name (Option C) and the operating system are gathered via DHCP fingerprinting, not layer 2 polling.

NEW QUESTION # 61
Refer to the exhibit.
FortiAnalyzer report



A FortiAnalyzer report is shown.
You must extract relevant information provided by the report regarding your OT network.
Which two statements are correct? (Choose two.)

- A. The report covers the last day.
- B. The attacks are blocked.

- C. Mobdus traffic is reported.
- D. The targeted IP address of the attacks is 10.1.5.1.

Answer: A,B

Explanation:
The report title indicates a daily summary with a defined one-day time range. The Top Threat section shows incidents categorized as blocked, confirming that the detected attacks were blocked.

NEW QUESTION # 62
.....