Free Questions for NSE7_OTS-7.2 by braindumpscollection

Shared by Rosales on 09-08-2024

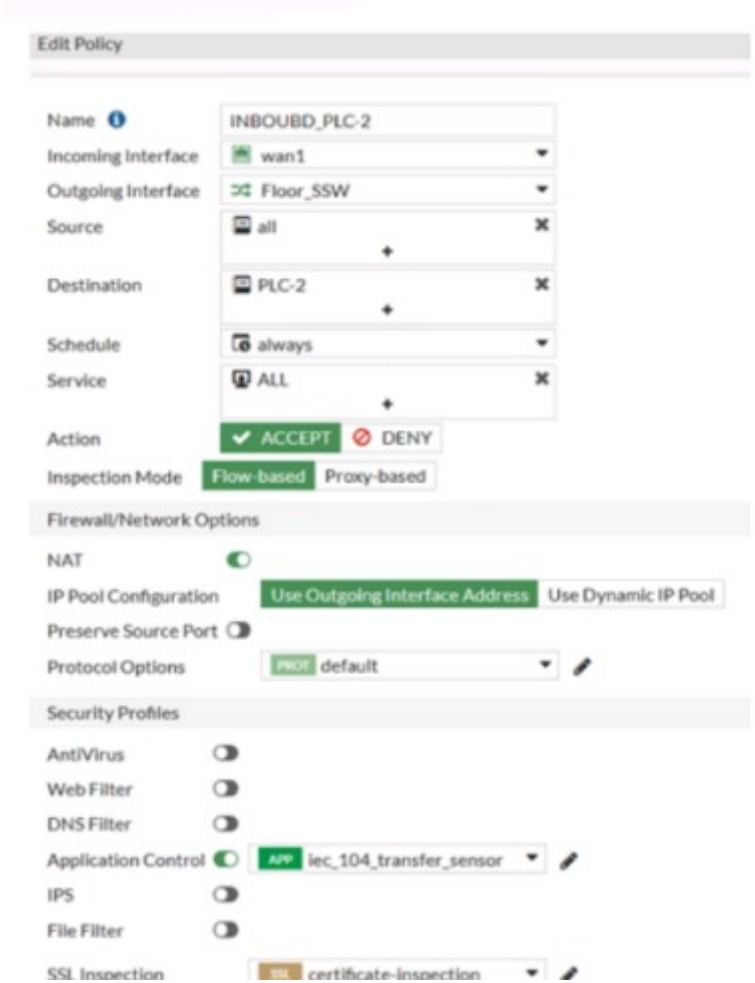
For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Refer to the exhibits.



Which statement is true about the traffic passing through to PLC-2?

Options:

A- IPS must be enabled to inspect application signatures.

B- The application filter overrides the default action of some IEC 104 signatures.

C- IEC 104 signatures are all allowed except the C.BO.NA 1 signature.

D- SSL Inspection must be set to deep-inspection to correctly apply application control.

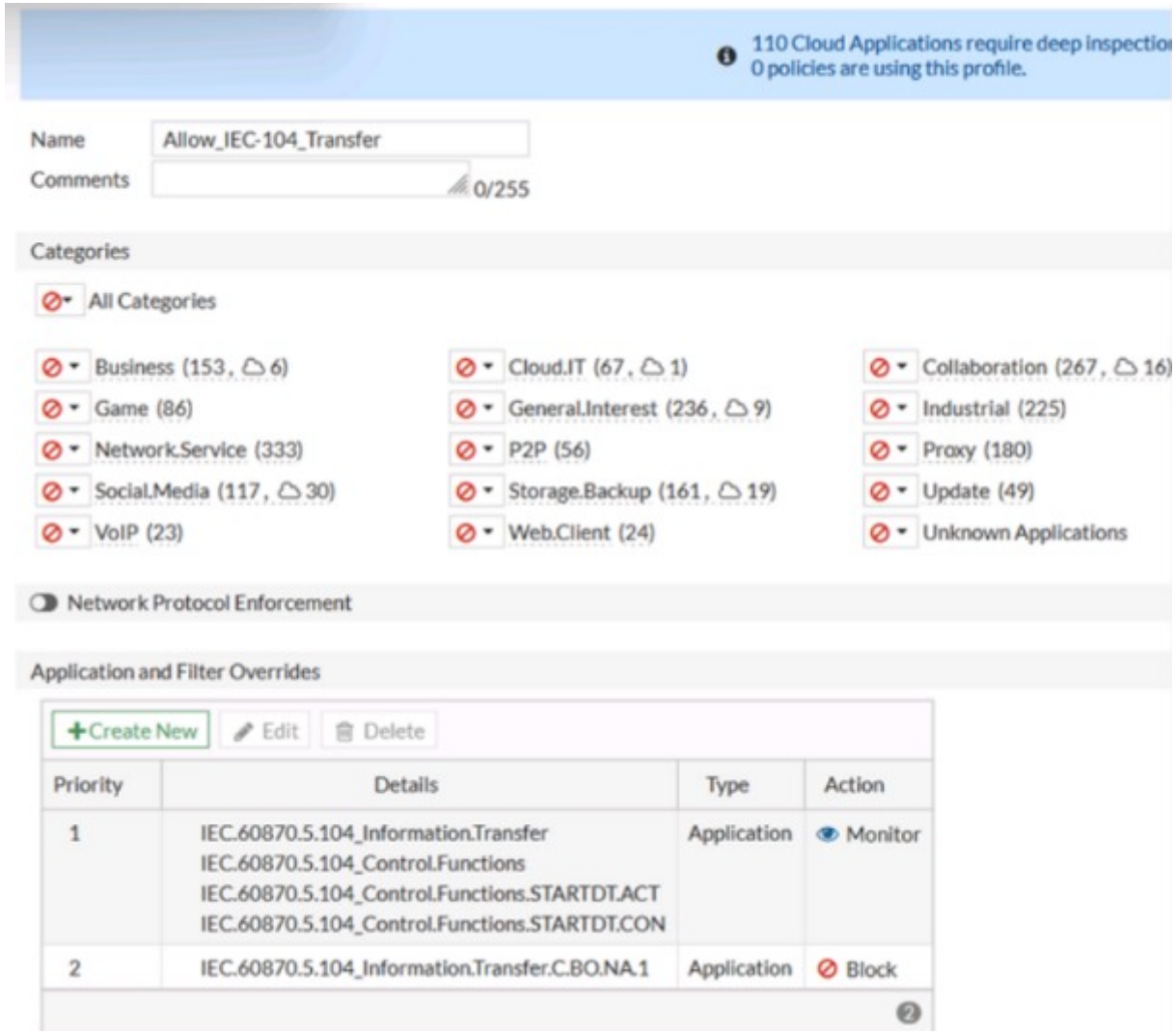
Answer:

B

Question 2

Question Type: MultipleChoice

Refer to the exhibit.



An OT network security audit concluded that the application sensor requires changes to ensure the correct security action is committed against the overrides filters.

Which change must the OT network administrator make?

Options:

A- Set all application categories to apply default actions.

B- Change the security action of the industrial category to monitor.

C- Set the priority of the C.BO.NA.1 signature override to 1.

D- Remove IEC.60870.5.104 Information.Transfer from the first filter override.

Answer:

D

Explanation:

According to the Fortinet NSE 7 - OT Security 6.4 exam guide1, the application sensor settings allow you to configure the security action for each application category and network protocol override. The security action determines how the FortiGate unit handles traffic that matches the application category or network protocol override. The security action can be one of the following:

Allow: The FortiGate unit allows the traffic without any further inspection.

Monitor: The FortiGate unit allows the traffic and logs it for monitoring purposes.

Block: The FortiGate unit blocks the traffic and logs it as an attack.

The priority of the network protocol override determines the order in which the FortiGate unit applies the security action to the traffic. The lower the priority number, the higher the priority. For example, a priority of 1 is higher than a priority of 10.

In the exhibit, the application sensor has the following settings:

The industrial category has a security action of allow, which means that the FortiGate unit will not inspect or log any traffic that belongs to this category.

The IEC.60870.5.104 Information.Transfer network protocol override has a security action of block, which means that the FortiGate unit will block and log any traffic that matches this protocol.

The IEC.60870.5.104 Control.Functions network protocol override has a security action of monitor, which means that the FortiGate unit will allow and log any traffic that matches this protocol.

The IEC.60870.5.104 Start/Stop network protocol override has a security action of allow, which means that the FortiGate unit will not inspect or log any traffic that matches this protocol.

The IEC.60870.5.104 Transfer.C.BO.NA.1 network protocol override has a security action of block, which means that the FortiGate unit will block and log any traffic that matches this protocol.

The problem with these settings is that the IEC.60870.5.104 Transfer.C.BO.NA.1 network protocol override has a lower priority than the IEC.60870.5.104 Information.Transfer network protocol override. This means that if the traffic matches both protocols, the FortiGate unit will apply the security action of the higher priority override, which is block. However, the IEC.60870.5.104 Transfer.C.BO.NA.1 protocol is used to transfer binary outputs, which are essential for controlling OT devices. Therefore, blocking this protocol could have negative consequences for the OT network.

To fix this issue, the OT network administrator must set the priority of the IEC.60870.5.104 Transfer.C.BO.NA.1 network protocol override to 1, which is higher than the priority of the IEC.60870.5.104 Information.Transfer network protocol override. This way, the FortiGate unit will apply the security action of the lower priority override, which is allow, to the traffic that matches both protocols. This will ensure that the FortiGate unit does not block the traffic that is used to transfer binary outputs, while still blocking the traffic that is used to transfer information.

1:NSE 7 Network Security Architect - Fortinet

Question 3

Question Type: **MultipleChoice**

As an OT network administrator, you are managing three FortiGate devices that each protect different levels on the Purdue model. To increase traffic visibility, you are required to implement additional security measures to detect exploits that affect PLCs.

Which security sensor must implement to detect these types of industrial exploits?

Options:

A- Intrusion prevention system (IPS)

B- Deep packet inspection (DPI)

C- Antivirus inspection

D- Application control

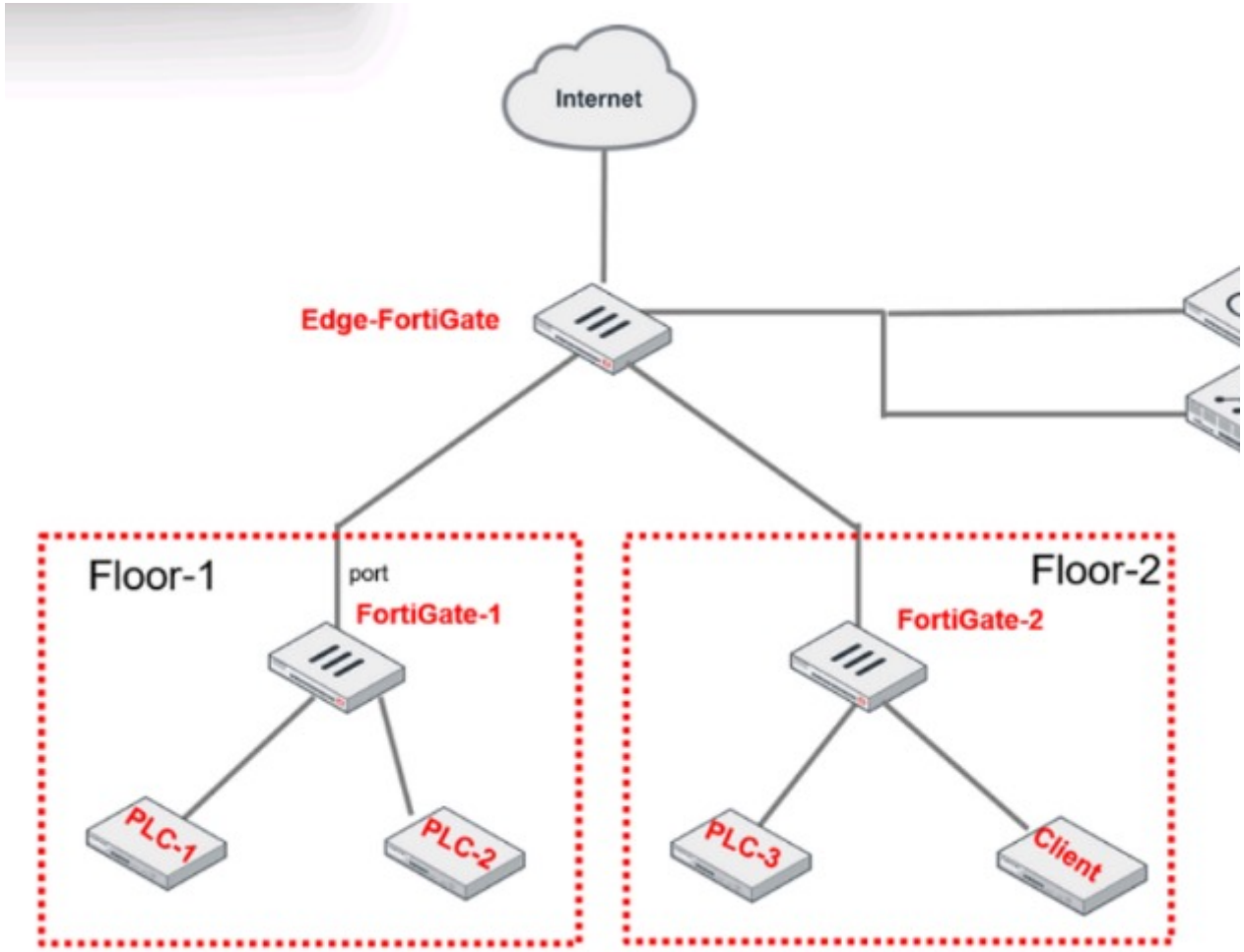
Answer:

D

Question 4

Question Type: **MultipleChoice**

Refer to the exhibit.



PLC-3 and CLIENT can send traffic to PLC-1 and PLC-2. FGT-2 has only one software switch (SSW-1) connecting both PLC-3 and CLIENT. PLC-3 and CLIENT can send traffic to each other at the Layer 2 level.

What must the OT admin do to prevent Layer 2-level communication between PLC-3 and CLIENT?

Options:

A- Set a unique forward domain for each interface of the software switch.

B- Create a VLAN for each device and replace the current FGT-2 software switch members.

C- Enable explicit intra-switch policy to require firewall policies on FGT-2.

D- Implement policy routes on FGT-2 to control traffic between devices.

Answer:

A, B

Question 5

Question Type: MultipleChoice

An OT network architect must deploy a solution to protect fuel pumps in an industrial remote network. All the fuel pumps must be closely monitored from the corporate network for any temperature fluctuations.

How can the OT network architect achieve this goal?

Options:

A- Configure a fuel server on the remote network, and deploy a FortiSIEM with a single pattern temperature security rule on the corporate network.

B- Configure a fuel server on the corporate network, and deploy a FortiSIEM with a single pattern temperature performance rule on the remote network.

C- Configure a fuel server on the remote network, and deploy a FortiSIEM with a single pattern temperature performance rule on the corporate network.

D- Configure both fuel server and FortiSIEM with a single-pattern temperature performance rule on the corporate network.

Answer:

C

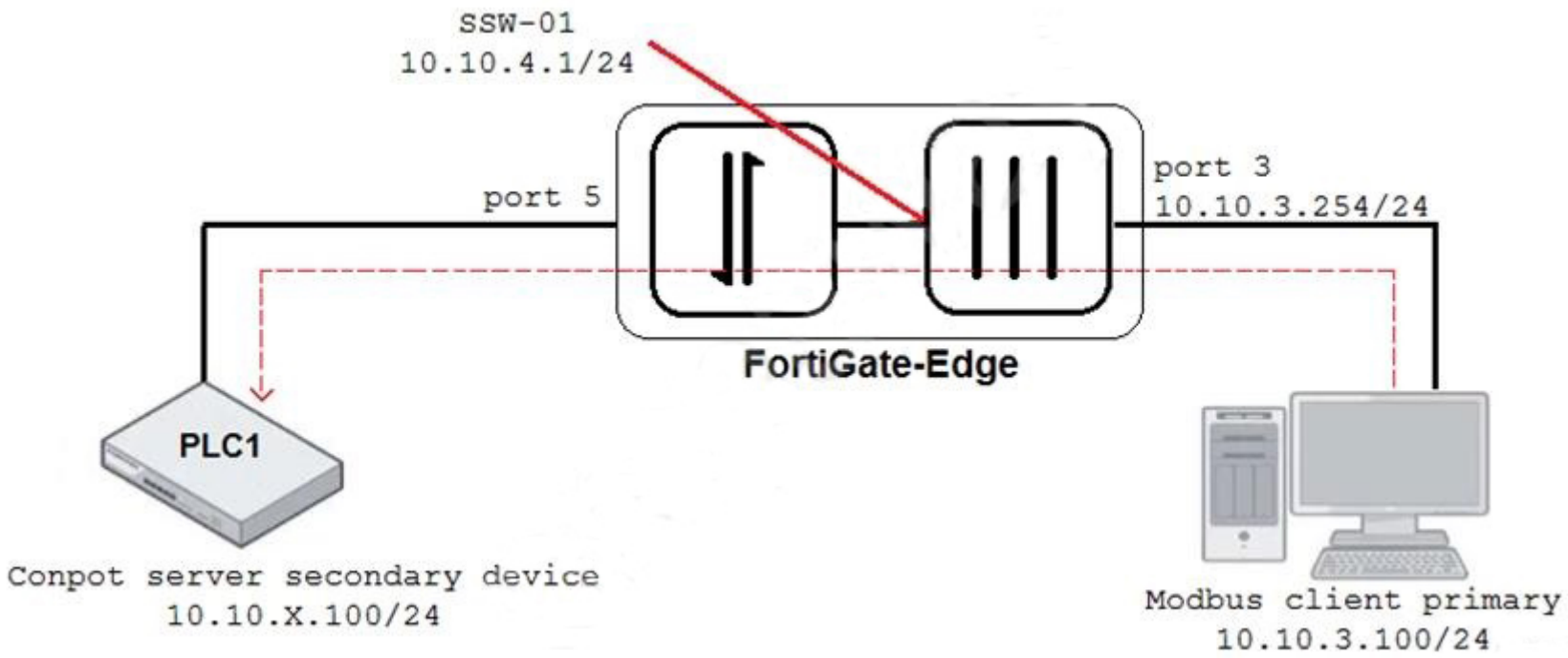
Explanation:

This way, FortiSIEM can discover and monitor everything attached to the remote network and provide security visibility to the corporate network

Question 6

Question Type: MultipleChoice

Refer to the exhibit.



An OT architect has implemented a Modbus TCP with a simulation server Conpot to identify and control the Modus traffic in the OT network. The FortiGate-Edge device is configured with a software switch interface ssw-01.

Based on the topology shown in the exhibit, which two statements about the successful simulation of traffic between client and server are true? (Choose two.)

Options:

A- The FortiGate-Edge device must be in NAT mode.

B- NAT is disabled in the FortiGate firewall policy from port3 to ssw-01.

C- The FortiGate devices is in offline IDS mode.

D- Port5 is not a member of the software switch.

Answer:

A, B

Question 7

Question Type: MultipleChoice

As an OT administrator, it is important to understand how industrial protocols work in an OT network.

Which communication method is used by the Modbus protocol?

Options:

A- It uses OSI Layer 2 and the primary device sends data based on request from secondary device.

B- It uses OSI Layer 2 and both the primary/secondary devices always send data during the communication.

C- It uses OSI Layer 2 and both the primary/secondary devices send data based on a matching token ring.

D- It uses OSI Layer 2 and the secondary device sends data based on request from primary device.

Answer:

D

Question 8

Question Type: MultipleChoice

What can be assigned using network access control policies?

Options:

A- Layer 3 polling intervals

B- FortiNAC device polling methods

C- Logical networks

D- Profiling rules

Answer:

C