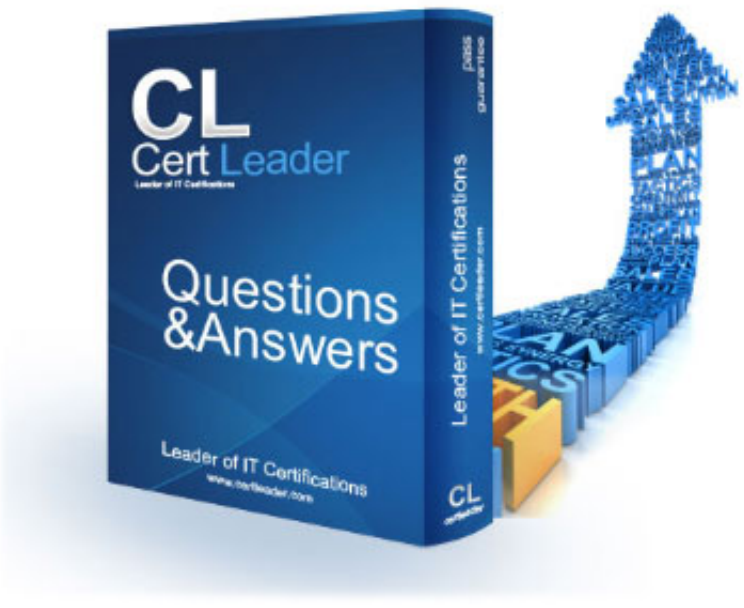
NSE7_OTS-7.2 Dumps

Fortinet NSE 7 - OT Security 7.2

https://www.certleader.com/NSE7_OTS-7.2-dumps.html



NEW QUESTION 1
When device profiling rules are enabled, which devices connected on the network are evaluated by the device profiling rules?

A. Known trusted devices, each time they change location
B. All connected devices, each time they connect
C. Rogue devices, only when they connect for the first time
D. Rogue devices, each time they connect

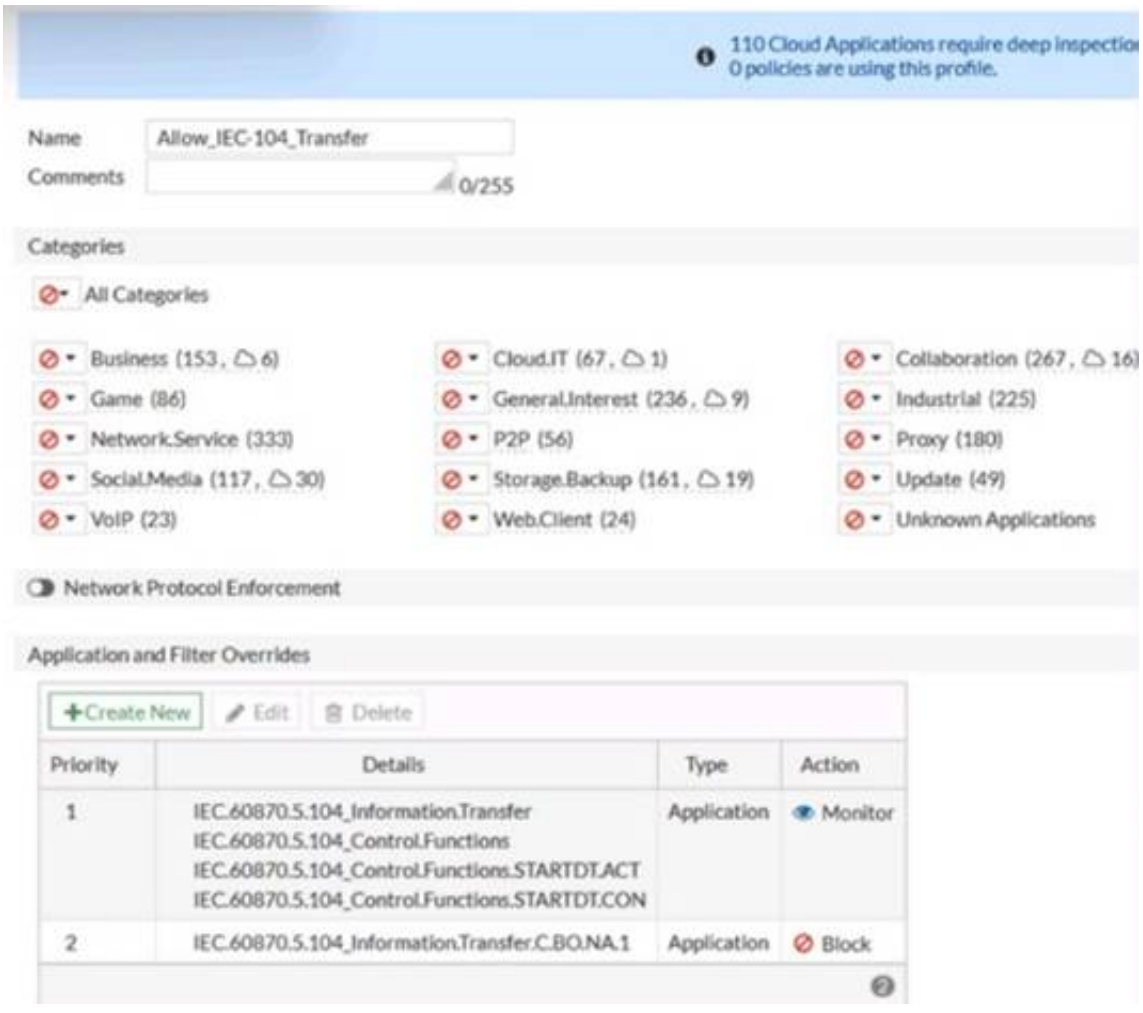
Answer: C

NEW QUESTION 2
To increase security protection in an OT network, how does application control on ForliGate detect industrial traffic?

A. By inspecting software and software-based vulnerabilities
B. By inspecting applications only on nonprotected traffic
C. By inspecting applications with more granularity by inspecting subapplication traffic
D. By inspecting protocols used in the application traffic

Answer: B

NEW QUESTION 3
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?

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: C

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 andnetwork 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

NEW QUESTION 4
Which type of attack posed by skilled and malicious users of security level 4 (SL 4) of IEC 62443 is designed to defend against intentional attacks?

A. Users with access to moderate resources
B. Users with low access to resources
C. Users with unintentional operator error
D. Users with substantial resources

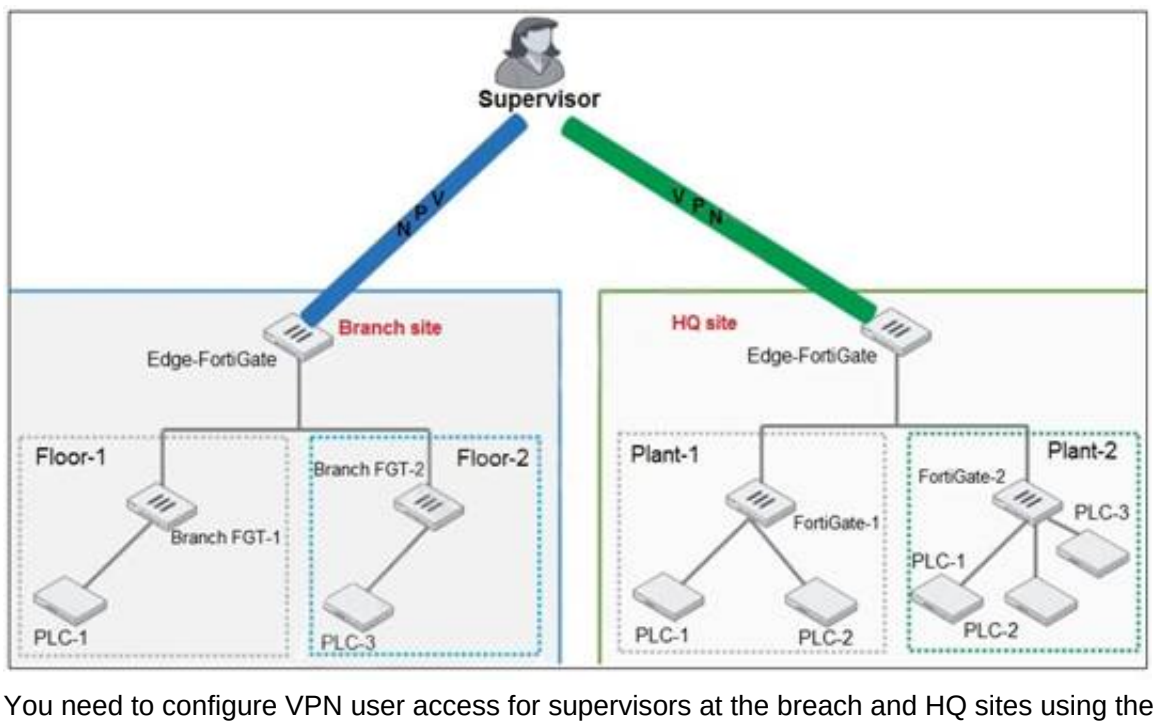
Answer: C

NEW QUESTION 5
An OT administrator has configured FSSO and local firewall authentication. A user who is part of a user group is not prompted from credentials during authentication.
What is a possible reason?

A. FortiGate determined the user by passive authentication
B. The user was determined by Security Fabric
C. Two-factor authentication is not configured with RADIUS authentication method
D. FortiNAC determined the user by DHCP fingerprint method

Answer: A

NEW QUESTION 6
Refer to the exhibit.



You need to configure VPN user access for supervisors at the breach and HQ sites using the same soft FortiToken. Each site has a FortiGate VPN gateway.
What must you do to achieve this objective?

A. You must use a FortiAuthenticator.
B. You must register the same FortiToken on more than one FortiGate.
C. You must use the user self-registration server.
D. You must use a third-party RADIUS OTP server.

Answer: A

NEW QUESTION 7
Which three common breach points can be found in a typical OT environment? (Choose three.)

A. Global hat
B. Hard hat
C. VLAN exploits
D. Black hat
E. RTU exploits

Answer: BDE

NEW QUESTION 8

An OT architect has deployed a Layer 2 switch in the OT network at Level 1 the Purdue model-process control. The purpose of the Layer 2 switch is to segment traffic between PLC1 and PLC2 with two VLANs. All the traffic between PLC1 and PLC2 must first flow through the Layer 2 switch and then through the FortiGate device in the Level 2 supervisory control network.
What statement about the traffic between PLC1 and PLC2 is true?

A. The Layer 2 switch rewrites VLAN tags before sending traffic to the FortiGate device.
B. The Layer 2 switches routes any traffic to the FortiGate device through an Ethernet link.
C. PLC1 and PLC2 traffic must flow through the Layer-2 switch trunk link to the FortiGate device.
D. In order to communicate, PLC1 must be in the same VLAN as PLC2.

Answer: C

Explanation:
The statement that is true about the traffic between PLC1 and PLC2 is that PLC1 and PLC2 traffic must flow through the Layer-2 switch trunk link to the FortiGate device.

NEW QUESTION 9
An administrator wants to use FortiSoC and SOAR features on a FortiAnalyzer device to detect and block any unauthorized access to FortiGate devices in an OT network.
Which two statements about FortiSoC and SOAR features on FortiAnalyzer are true? (Choose two.)

A. You must set correct operator in event handler to trigger an event.
B. You can automate SOC tasks through playbooks.
C. Each playbook can include multiple triggers.
D. You cannot use Windows and Linux hosts security events with FortiSoC.

Answer: AB

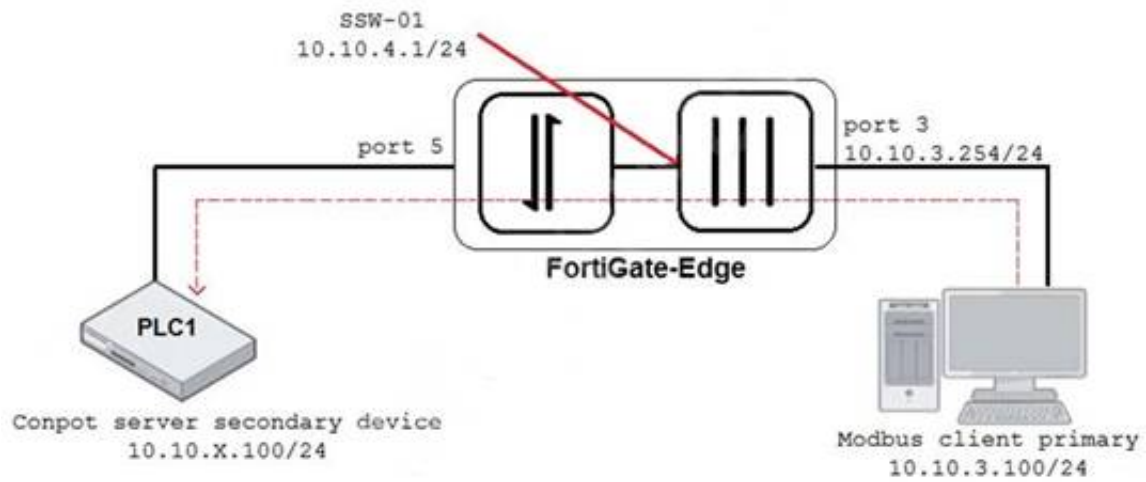
Explanation:
Ref: https://docs.fortinet.com/document/fortianalyzer/7.0.0/administration-guide/268882/fortisoc

NEW QUESTION 10
Which two statements are true when you deploy FortiGate as an offline IDS? (Choose two.)

A. FortiGate receives traffic from configured port mirroring.
B. Network traffic goes through FortiGate.
C. FortiGate acts as network sensor.
D. Network attacks can be detected and blocked.

Answer: BC

NEW QUESTION 10
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.)

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: AB

NEW QUESTION 12
In a wireless network integration, how does FortiNAC obtain connecting MAC address information?

A. RADIUS
B. Link traps
C. End station traffic monitoring
D. MAC notification traps

Answer: A

Explanation:
FortiNAC can integrate with RADIUS servers to obtain MAC address information for wireless clients that authenticate through the RADIUS server. Reference: Fortinet NSE 7 - OT Security 6.4 Study Guide, Chapter 4: OT Security Devices, page 4-28.

NEW QUESTION 14
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your NSE7_OTS-7.2 Exam with Our Prep Materials Via below:

https://www.certleader.com/NSE7_OTS-7.2-dumps.html