

NSE7_OTIS-7.2 Dumps

Fortinet NSE 7 - OT Security 7.2

https://www.certleader.com/NSE7_OTIS-7.2-dumps.html



NEW QUESTION 1

Refer to the exhibit.

Device Name	Device Type	Vendor	Device Type Model	Device Hardware Model	Device Image File	Count
SJ-QA-A-IOS-JunOffice	Cisco		IOS	1760	C1700-advsecurity9-mz.123-8.T4.bin	1
SJ-Main-Cat6500	Cisco		IOS	WS-C6509	s72033-advservicesk9_wan-mz.122-33.SX01.bin	1
ph-network-3560_1	Cisco		IOS	WS-C3560G-48PS-S	c3560-advservicesk9-mz.122-25.SEE4.bin	1

An OT administrator ran a report to identify device inventory in an OT network. Based on the report results, which report was run?

- A. A FortiSIEM CMDB report
- B. A FortiAnalyzer device report
- C. A FortiSIEM incident report
- D. A FortiSIEM analytics report

Answer: A

NEW QUESTION 2

Refer to the exhibit.



Based on the Purdue model, which three measures can be implemented in the control area zone using the Fortinet Security Fabric? (Choose three.)

- A. FortiGate for SD-WAN
- B. FortiGate for application control and IPS
- C. FortiNAC for network access control
- D. FortiSIEM for security incident and event management
- E. FortiEDR for endpoint detection

Answer: BCE

NEW QUESTION 3

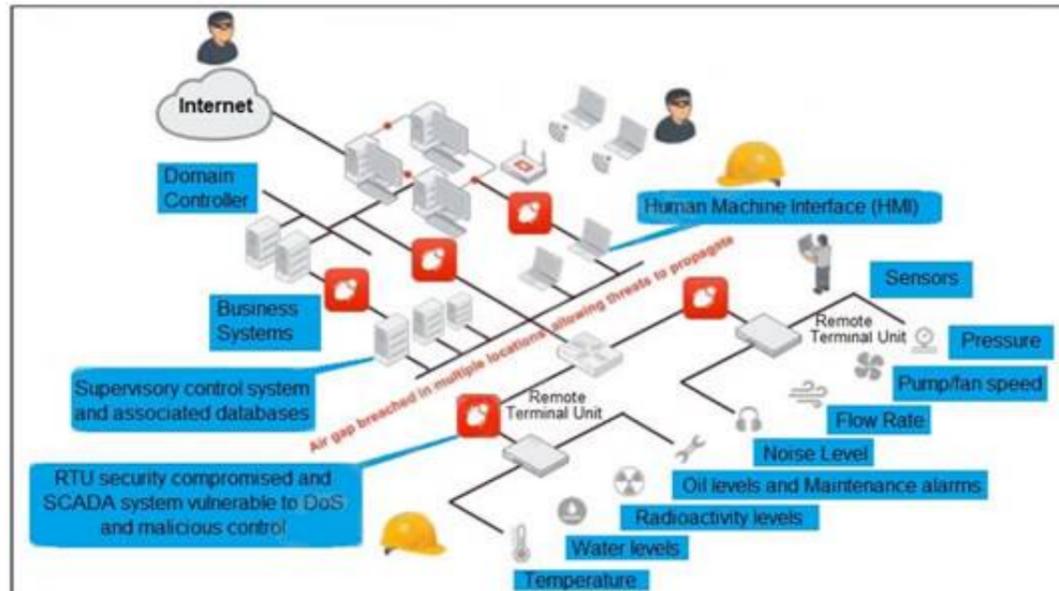
To increase security protection in an OT network, how does application control on FortiGate detect industrial traffic?

- 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 4

Refer to the exhibit, which shows a non-protected OT environment.



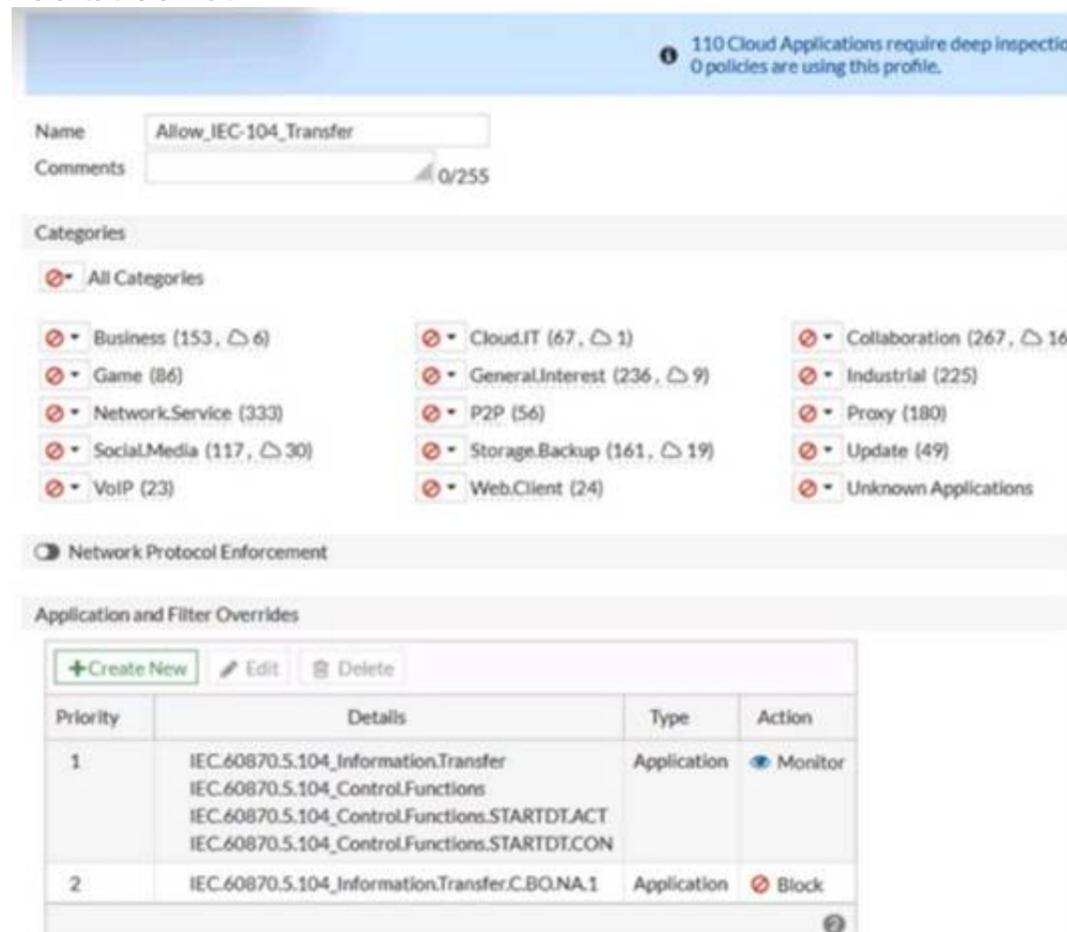
An administrator needs to implement proper protection on the OT network.
Which three steps should an administrator take to protect the OT network? (Choose three.)

- A. Deploy an edge FortiGate between the internet and an OT network as a one-arm sniffer.
- B. Deploy a FortiGate device within each ICS network.
- C. Configure firewall policies with web filter to protect the different ICS networks.
- D. Configure firewall policies with industrial protocol sensors
- E. Use segmentation

Answer: ACD

NEW QUESTION 5

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 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

NEW QUESTION 6

The OT network analyst runs different level of reports to quickly explore threats that exploit the network. Such reports can be run on all routers, switches, and firewalls. Which FortiSIEM reporting method helps to identify these type of exploits of image firmware files?

- A. CMDB reports
- B. Threat hunting reports
- C. Compliance reports
- D. OT/IoT reports

Answer: B

NEW QUESTION 7

An OT network administrator is trying to implement active authentication. Which two methods should the administrator use to achieve this? (Choose two.)

- A. Two-factor authentication on FortiAuthenticator
- B. Role-based authentication on FortiNAC
- C. FSSO authentication on FortiGate
- D. Local authentication on FortiGate

Answer: AD

NEW QUESTION 8

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?

- A. Intrusion prevention system (IPS)
- B. Deep packet inspection (DPI)
- C. Antivirus inspection
- D. Application control

Answer: B

NEW QUESTION 9

What two advantages does FortiNAC provide in the OT network? (Choose two.)

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

Answer: AD

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 10

Refer to the exhibit.

```
config system interface
  edit VLAN101_dmz
    set forward-domain 101
  next
  edit VLAN101_internal
    set forward-domain 101
end
```

Given the configurations on the FortiGate, which statement is true?

- A. FortiGate is configured with forward-domains to reduce unnecessary traffic.
- B. FortiGate is configured with forward-domains to forward only domain controller traffic.
- C. FortiGate is configured with forward-domains to forward only company domain website traffic.
- D. FortiGate is configured with forward-domains to filter and drop non-domain controller traffic.

Answer: A

NEW QUESTION 10

.....

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_OTIS-7.2 Exam with Our Prep Materials Via below:

https://www.certleader.com/NSE7_OTIS-7.2-dumps.html