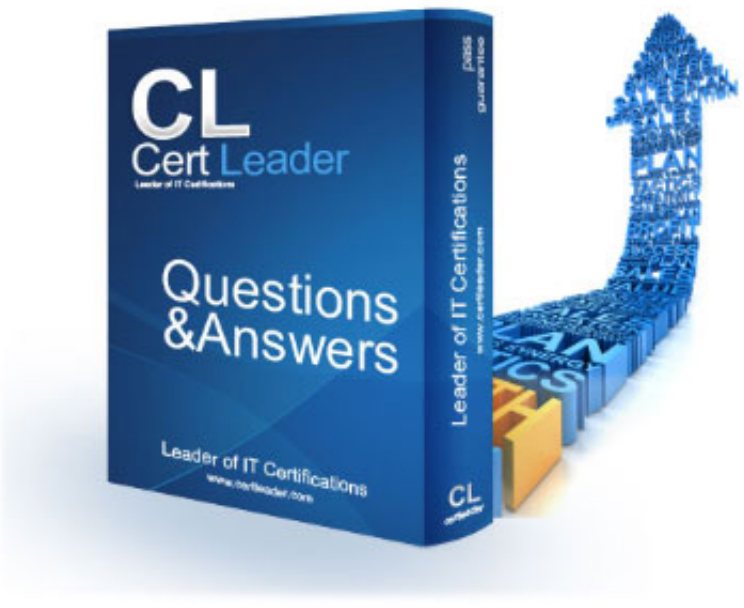
NSE7_OTS-6.4 Dumps

Fortinet NSE 7 - OT Security 6.4

https://www.certleader.com/NSE7_OTS-6.4-dumps.html



NEW QUESTION 1
An OT supervisor needs to protect their network by implementing security with an industrial signature database on the FortiGate device.
Which statement about the industrial signature database on FortiGate is true?

A. A supervisor must purchase an industrial signature database and import it to the FortiGate.
B. An administrator must create their own database using custom signatures.
C. By default, the industrial database is enabled.
D. A supervisor can enable it through the FortiGate CLI.

Answer: D

NEW QUESTION 2
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: BC

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

NEW QUESTION 3
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?

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

NEW QUESTION 4
What triggers Layer 2 polling of infrastructure devices connected in the network?

A. A failed Layer 3 poll
B. A matched security policy
C. A matched profiling rule
D. A linkup or linkdown trap

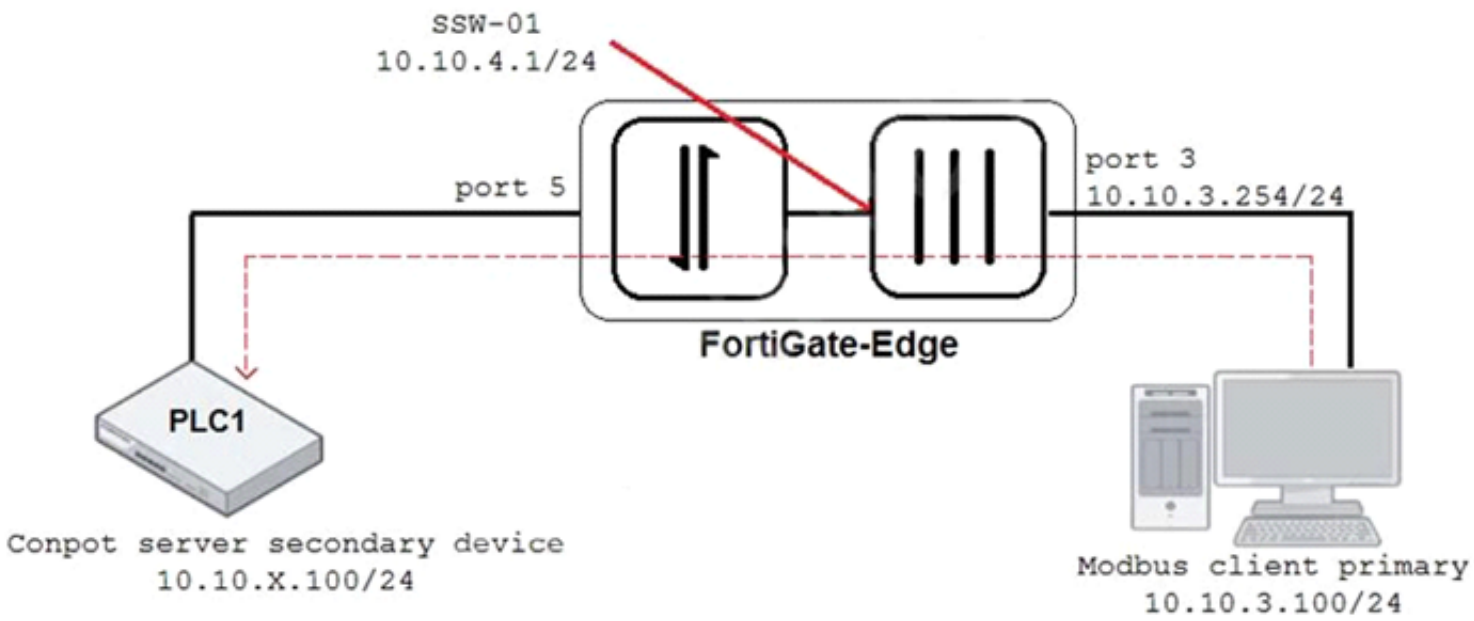
Answer: D

NEW QUESTION 5
Which three Fortinet products can be used for device identification in an OT industrial control system (ICS)? (Choose three.)

A. FortiNAC
B. FortiManager
C. FortiAnalyzer
D. FortiSIEM
E. FortiGate

Answer: ACD

NEW QUESTION 6
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.

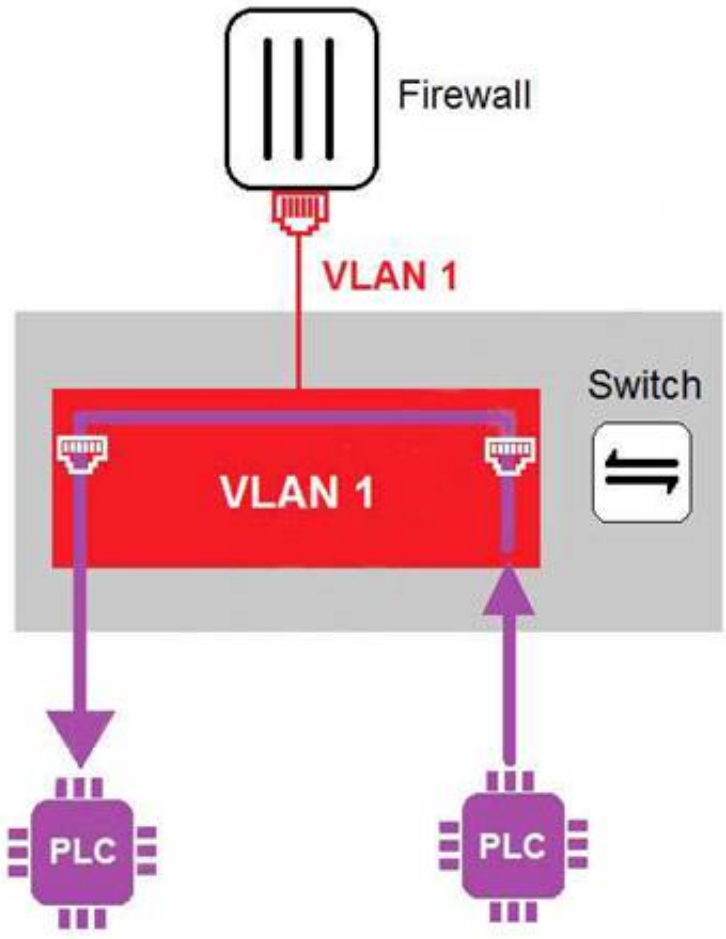
Answer: AC

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: AB

NEW QUESTION 8
Refer to the exhibit

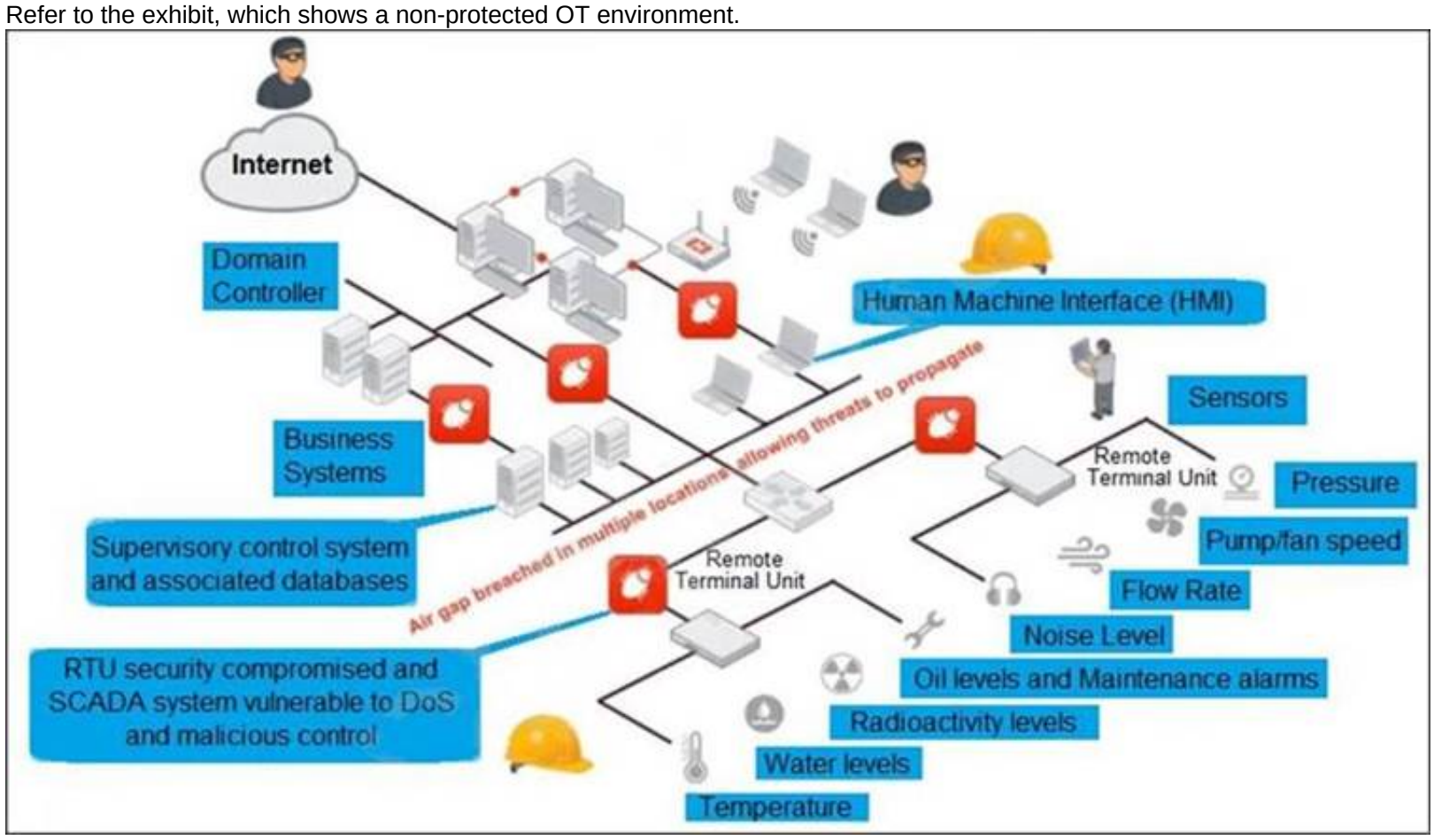


In the topology shown in the exhibit, both PLCs can communicate directly with each other, without going through the firewall.
Which statement about the topology is true?

A. PLCs use IEEE802.1Q protocol to communicate each other.
B. An administrator can create firewall policies in the switch to secure between PLCs.
C. This integration solution expands VLAN capabilities from Layer 2 to Layer 3.
D. There is no micro-segmentation in this topology.

Answer: D

NEW QUESTION 9
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 10
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

NEW QUESTION 10
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 11
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 16
You are investigating a series of incidents that occurred in the OT network over past 24 hours in FortiSIEM. Which three FortiSIEM options can you use to investigate these incidents? (Choose three.)

A. Security
B. IPS
C. List
D. Risk
E. Overview

Answer: CDE

NEW QUESTION 21
.....

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-6.4 Exam with Our Prep Materials Via below:

https://www.certleader.com/NSE7_OTS-6.4-dumps.html