# Fortinet

## Exam Questions NSE7_OTS-6.4

Fortinet NSE 7 - OT Security 6.4

**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.

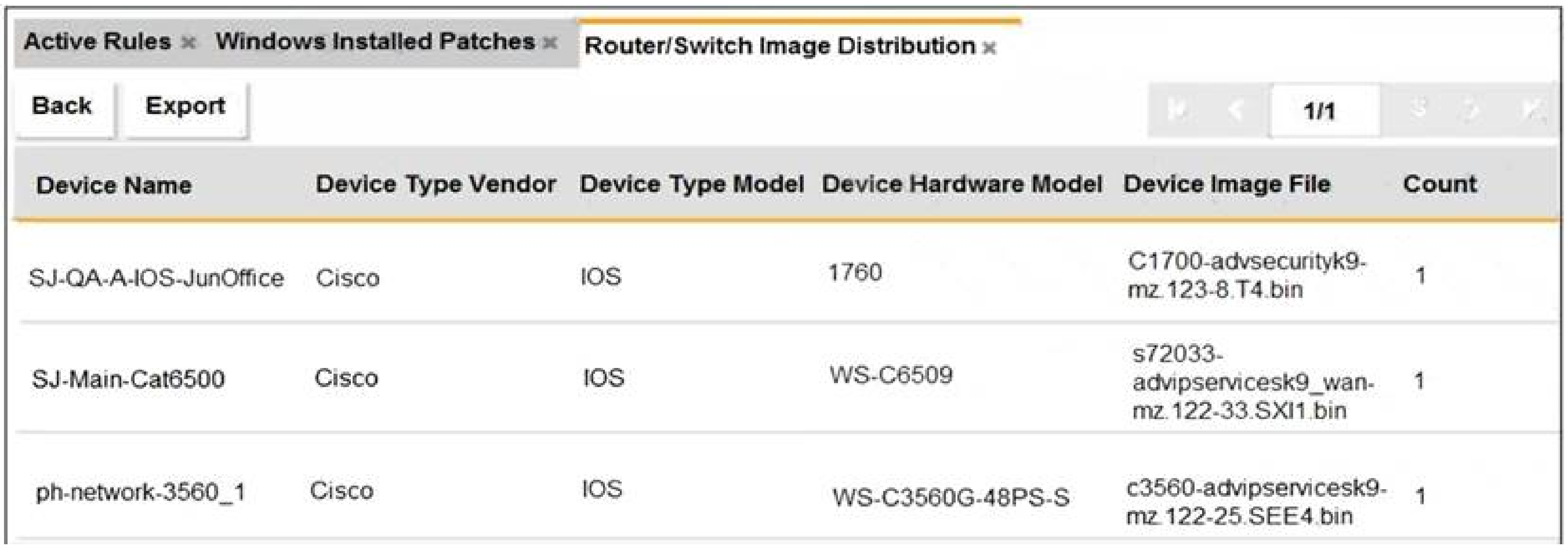
**Answer:** D

**NEW QUESTION 2**
When you create a user or host profile, which three criteria can you use? (Choose three.)

A. Host or user group memberships
B. Administrative group membership
C. An existing access control policy
D. Location
E. Host or user attributes

**Answer:** ADE

**NEW QUESTION 3**
Refer to the exhibit.


Active Rules ×
Windows Installed Patches ×
Router/Switch Image Distribution ×
Back
Export
1/1

| Device Name | Device Type Vendor | Device Type Model | Device Hardware Model | Device Image File | Count |
|---|---|---|---|---|---|
| SJ-QA-A-IOS-JunOffice | Cisco | IOS | 1760 | C1700-advsecurityk9-mz.123-8.T4.bin | 1 |
| SJ-Main-Cat6500 | Cisco | IOS | WS-C6509 | s72033-advipservicesk9_wan-mz.122-33.SXI1.bin | 1 |
| ph-network-3560_1 | Cisco | IOS | WS-C3560G-48PS-S | c3560-advipservicesk9-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 4**
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 5**
An OT supervisor has configured LDAP and FSSO for the authentication. The goal is that all the users be authenticated against passive authentication first and, if passive authentication is not successful, then users should be challenged with active authentication.
What should the OT supervisor do to achieve this on FortiGate?

A. Configure a firewall policy with LDAP users and place it on the top of list of firewall policies.
B. Enable two-factor authentication with FSSO.
C. Configure a firewall policy with FSSO users and place it on the top of list of firewall policies.
D. Under config user settings configure set auth-on-demand implicit.

**Answer:** D

**NEW QUESTION 6**
Which three methods of communication are used by FortiNAC to gather visibility information? (Choose three.)

A. SNMP
B. ICMP
C. API
D. RADIUS
E. TACACS

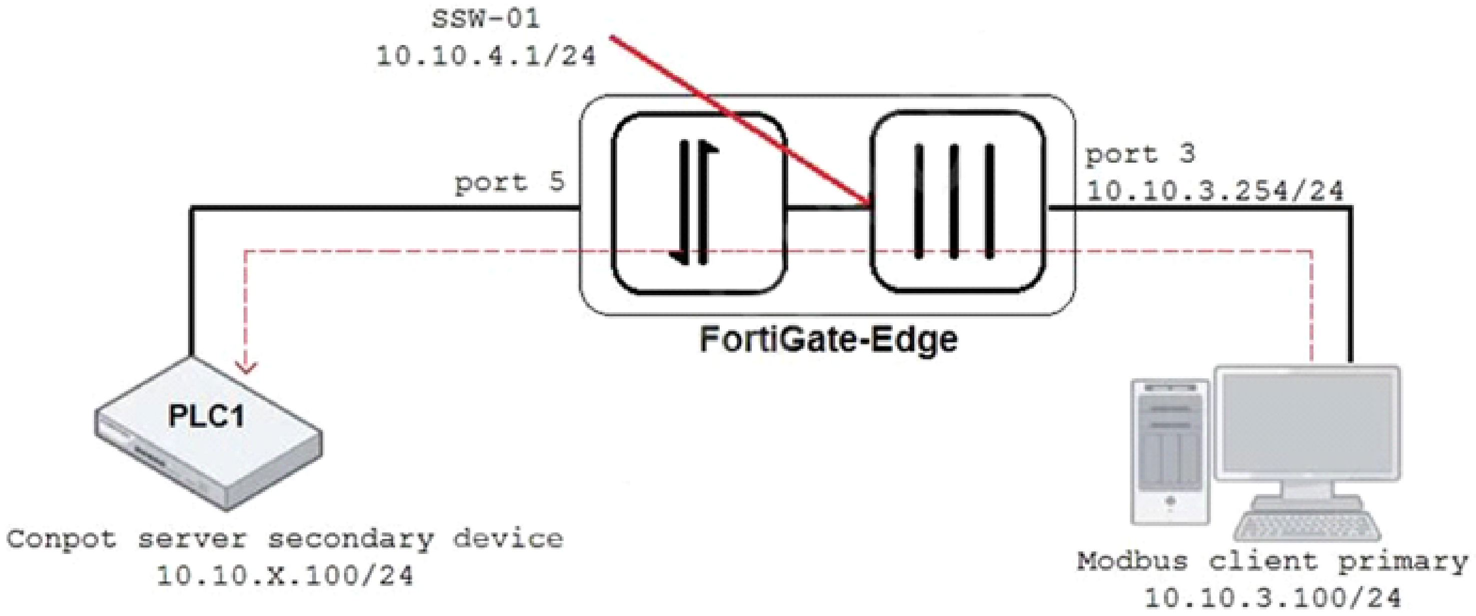
**Answer:** ACD

**NEW QUESTION 7**
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 8**
Refer to the exhibit.

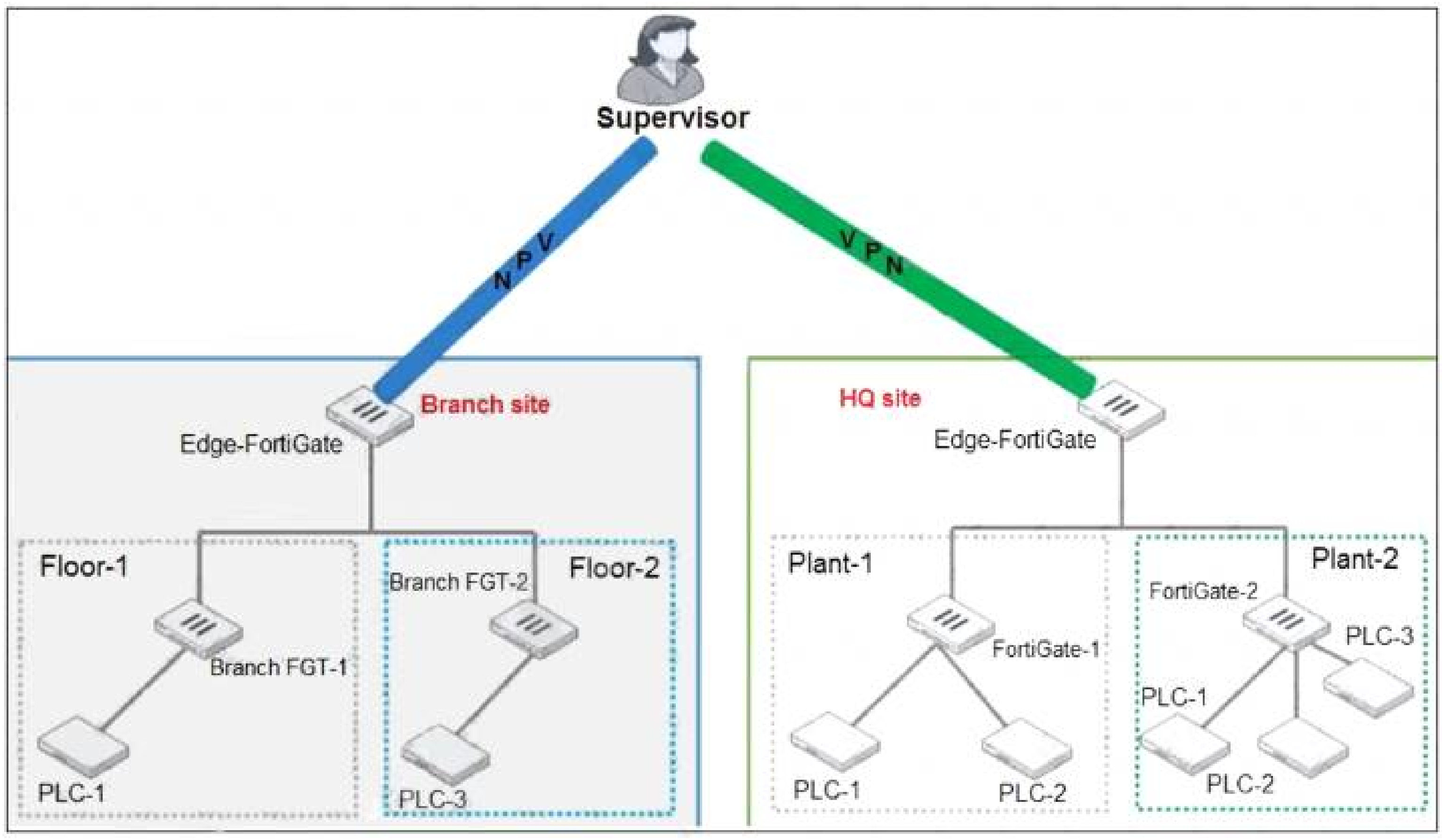


An OT architect has implemented a Modbus TCP with a simulation server Conpot to identify and control the Modus traffic in the OT network. The FortiGate-Edge device is configured with a software switch interface ssw-01.
Based on the topology shown in the exhibit, which two statements about the successful 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 9**
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.

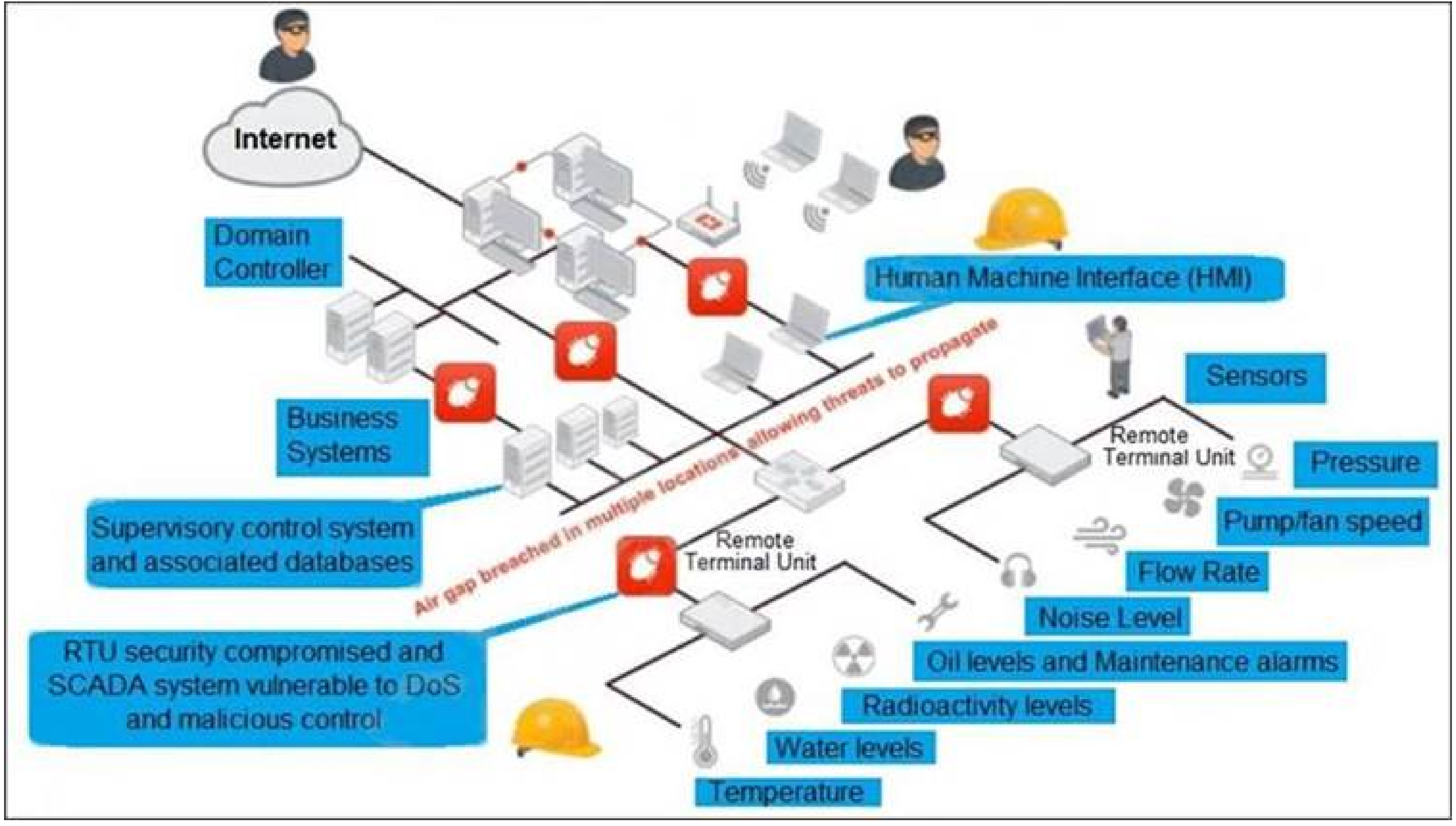
**Answer:** A

**NEW QUESTION 10**
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 10**
Refer to the exhibit, which shows a non-protected OT environment.


Internet
Domain Controller
Human Machine Interface (HMI)
Sensors
Business Systems
Remote Terminal Unit
Pressure
Pump/fan speed
Supervisory control system and associated databases
Air gap breached in multiple locations allowing threats to propagate
Remote Terminal Unit
Flow Rate
Noise Level
RTU security compromised and SCADA system vulnerable to DoS and malicious control
Oil levels and Maintenance alarms
Radioactivity levels
Water levels
Temperature

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

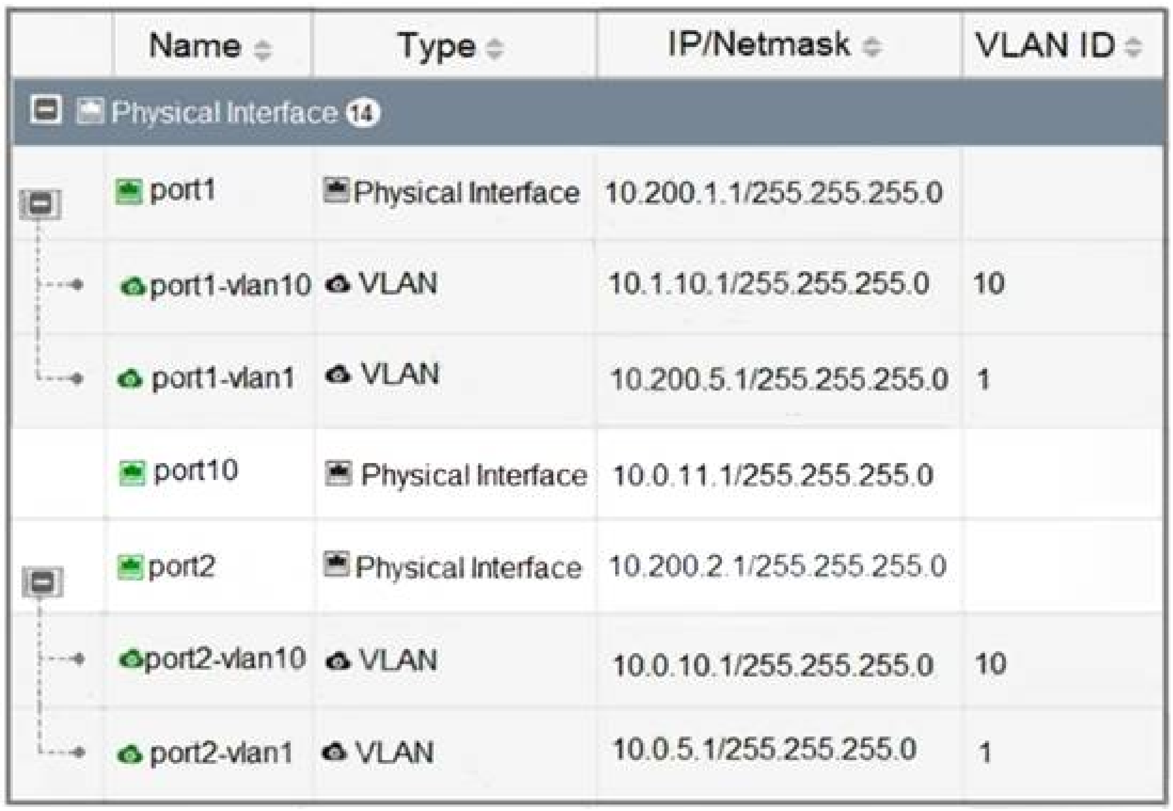
**Answer:** ACD

**NEW QUESTION 12**
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?

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:** B

**NEW QUESTION 15**
Refer to the exhibit.



| Name | Type | IP/Netmask | VLAN ID |
|---|---|---|---|
| Physical Interface 14 | | | |
| port1 | Physical Interface | 10.200.1.1/255.255.255.0 | |
| port1-vlan10 | VLAN | 10.1.10.1/255.255.255.0 | 10 |
| port1-vlan1 | VLAN | 10.200.5.1/255.255.255.0 | 1 |
| port10 | Physical Interface | 10.0.11.1/255.255.255.0 | |
| port2 | Physical Interface | 10.200.2.1/255.255.255.0 | |
| port2-vlan10 | VLAN | 10.0.10.1/255.255.255.0 | 10 |
| port2-vlan1 | VLAN | 10.0.5.1/255.255.255.0 | 1 |

Which statement about the interfaces shown in the exhibit is true?

A. port2, port2-vlan10, and port2-vlan1 are part of the software switch interface.
B. The VLAN ID of port1-vlan1 can be changed to the VLAN ID 10.
C. port1-vlan10 and port2-vlan10 are part of the same broadcast domain
D. port1, port1-vlan10, and port1-vlan1 are in different broadcast domains

**Answer:** D

**NEW QUESTION 17**
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 20**
An OT administrator is defining an incident notification policy using FortiSIEM and would like to configure the system with a notification policy. If an incident occurs, the administrator would like to be able to intervene and block an IP address or disable a user in Active Directory from FortiSIEM.
Which step must the administrator take to achieve this task?

A. Configure a fabric connector with a notification policy on FortiSIEM to connect with FortiGate.
B. Create a notification policy and define a script/remediation on FortiSIEM.
C. Define a script/remediation on FortiManager and enable a notification rule on FortiSIEM.
D. Deploy a mitigation script on Active Directory and create a notification policy on FortiSIEM.

**Answer:** C

**NEW QUESTION 25**
What can be assigned using network access control policies?

A. Layer 3 polling intervals
B. FortiNAC device polling methods
C. Logical networks
D. Profiling rules

**Answer:** D

**NEW QUESTION 30**
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 32**

......