

# **Fortinet**

## **NSE7\_OTS-7.2.0**

### **Fortinet NSE 6 - OT Security 7.2 Architect**



**For More Information – Visit link below:**

**<https://www.examsboost.com/>**

### **Product Version**

- ✓ Up to Date products, reliable and verified.
- ✓ Questions and Answers in PDF Format.

# Latest Version: 6.0

## Question: 1

Refer to the exhibit.

Active Rules x Windows Installed Patches x Router/Switch Image Distribution x						
Back Export		1/1 3				
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.SX11.bin	1	
ph-network-3560_1	Cisco	IOS	WS-C3560G-48PS-S	c3560-advipservicesk9-mz.122-25.SEE4.bin	1	

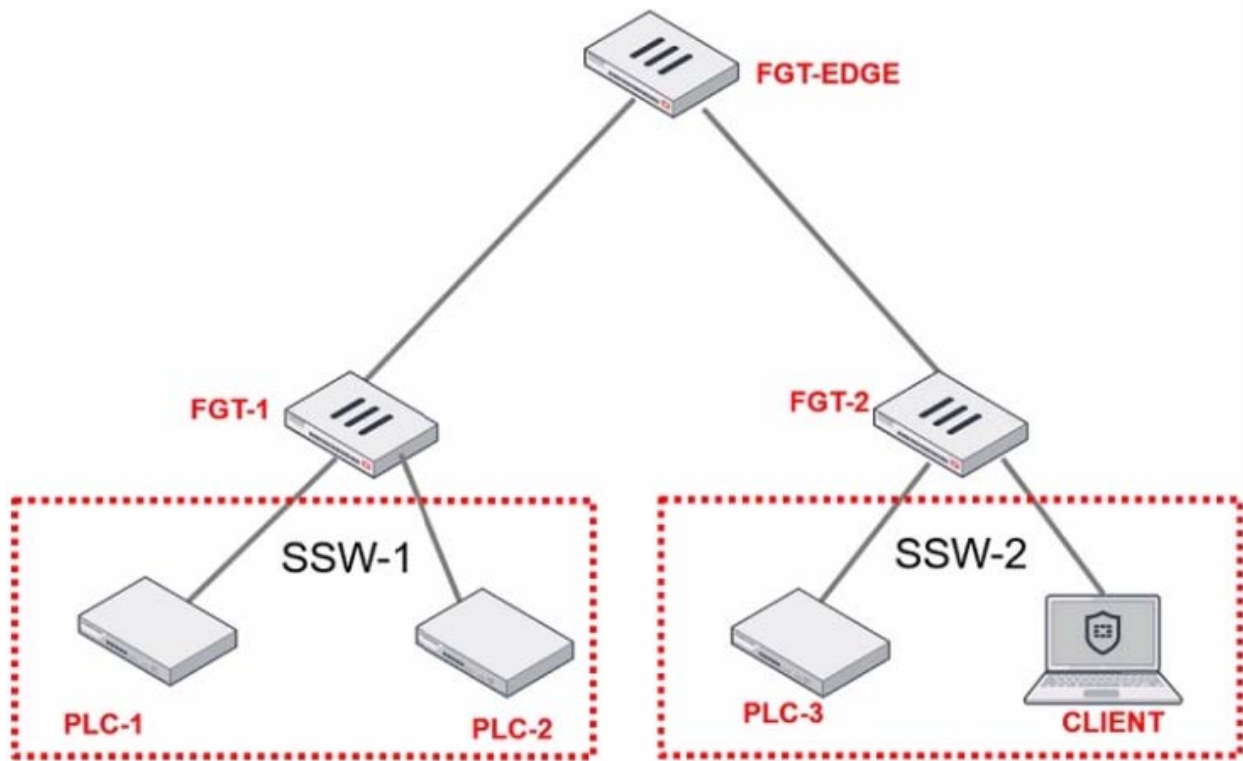
An OT administrator ran a report to identify device inventory in an OT network. Based on the report results, which report was run? (Choose one answer)

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

**Answer: A**

## Question: 2

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-2) connecting both PLC-3 and CLIENT. PLC-3 and CLIENT can send traffic to each other at the layer 2 level. What must the operational technology (OT) admin do to prevent layer 2-level communication between PLC-3 and CLIENT? (Choose one answer)

- A. Create a VLAN for each device and replace the current FGT-2 software switch members.
- B. Enable an explicit intra-switch policy to require firewall policies on FGT-2.
- C. Implement policy routes on FGT-2 to control traffic between devices.
- D. Set a unique forward domain for each interface of the software switch.

**Answer: B**

### Question: 3

The operational technology (OT) network analyst runs different levels of reports to investigate threats that exploit the network. The analyst can run these reports on all routers, switches, and firewalls.

Which FortiSIEM reporting method can analysts use to identify threats that exploit image firmware files? (Choose one answer)

- A. Threat hunting reports
- B. Payment card industry (PCI) logging reports
- C. Compliance reports
- D. Configuration management database (CMDB) reports

**Answer: D**

### Question: 4

Which two statements about the Modbus protocol are true? (Choose two answers)

- A. Modbus is used to establish communication between intelligent devices
- B. Most of the PLC brands come with a built-in Modbus module
- C. Modbus uses UDP frames to transport MBAP and function codes
- D. You can implement Modbus networking settings on internetworking devices

**Answer: A,B**

### Question: 5

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.

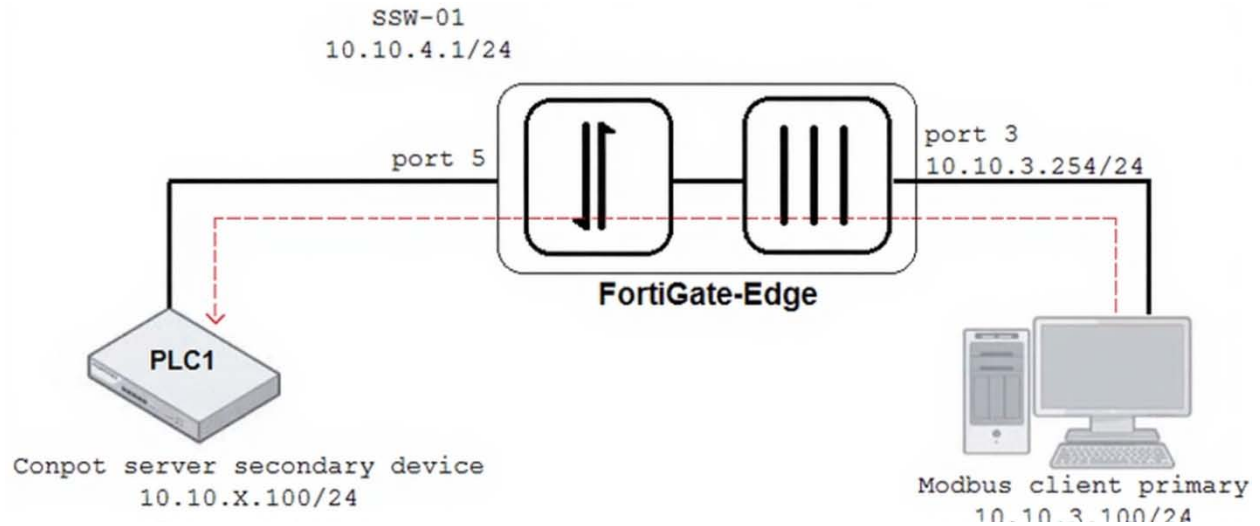
How can the OT network architect achieve this goal? (Choose one answer)

- 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**

### Question: 6

Refer to the exhibit.



An OT architect has implemented a Modbus TCP with a simulation server Conpot to identify and control the Modbus 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 answers)

- 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

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 answers)

- 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: B,C,E**

### Question: 8



When device profiling rules are enabled, which devices connected on the network are evaluated by the device profiling rules? (Choose one answer)

- 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: B**

### Question: 9

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? (Choose one answer)

- 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**

### Question: 10

When you create a user or host profile; which three criteria can you use? (Choose three answers)

- A. An applied (existing) access policy
- B. Administrative group membership
- C. Location
- D. Host or user group memberships
- E. Host or user attributes

**Answer: C,D,E**

# Thank You for Trying Our Product

For More Information – **Visit link below:**

**<https://www.examsboost.com/>**

15 USD Discount Coupon Code:

**G74JA8UF**

## FEATURES

- ✓ **90 Days Free Updates**
- ✓ **Money Back Pass Guarantee**
- ✓ **Instant Download or Email Attachment**
- ✓ **24/7 Live Chat Support**
- ✓ **PDF file could be used at any Platform**
- ✓ **50,000 Happy Customer**



Visit us at: <https://www.examsboost.com/test/nse7-ots-7-2-0>