FORTINET

NSE7_OTS-6.4

Fortinet NSE 7 - OT Security 6.4

E EXAMKILLER

Help Pass Your Exam At First Try

Fortinet

Exam NSE7_OTS-6.4

Fortinet NSE 7 - OT Security 6.4

Version: 3.1

[Total Questions: 35]

Question No : 1

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: C

Explanation: The OT supervisor should configure a firewall policy with FSSO users and place it on the top of list of firewall policies in order to achieve the goal of authenticating users against passive authentication first and, if passive authentication is not successful, then challenging them with active authentication.

Question No : 2

Refer to the exhibit.
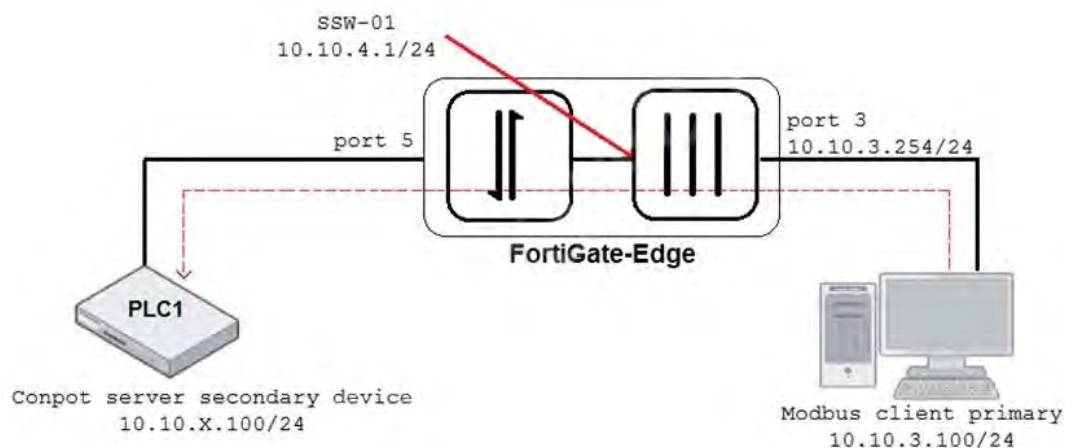
An OT architect has implemented a Modbus TCP with a simulation server Conpot to identify and control the Modus traffic in the OT network. The FortiGate-Edge device is configured with a software switch interface ssw-01.

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: A,B

Question No : 3

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

Question No : 4

Refer to the exhibit.
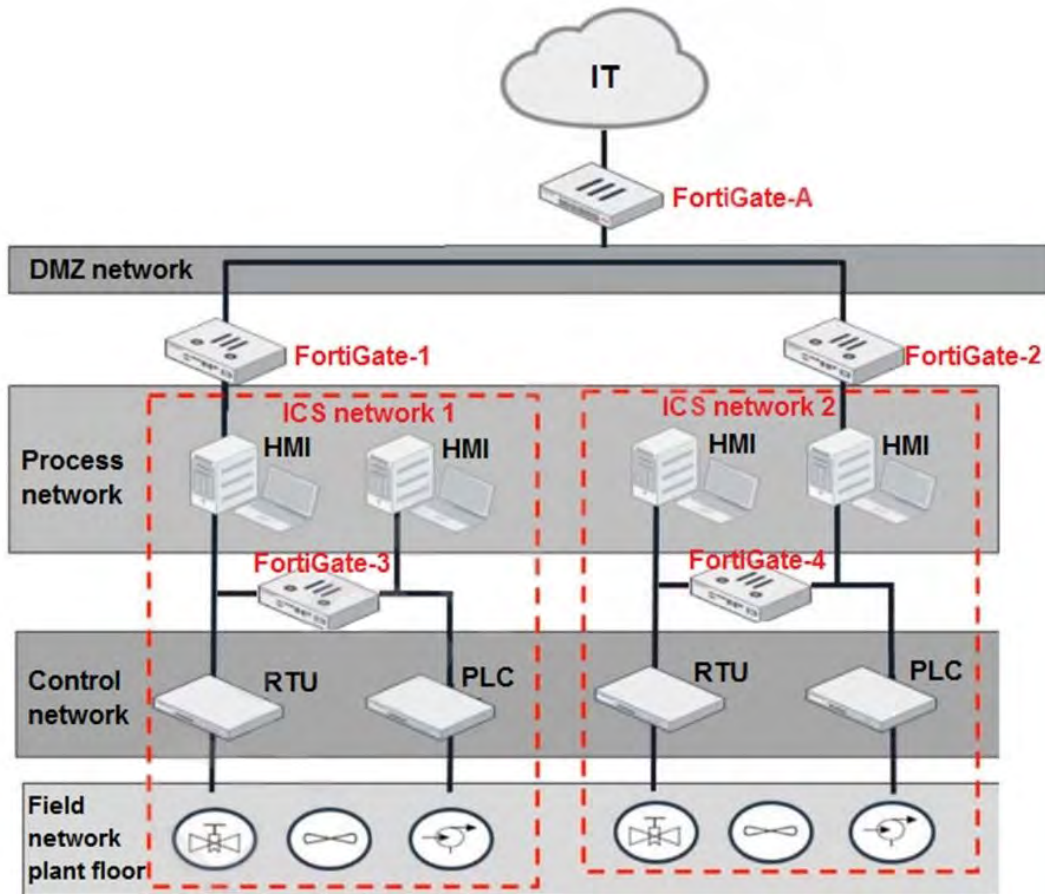
Based on the topology designed by the OT architect, which two statements about implementing OT security are true? (Choose two.)

A. Firewall policies should be configured on FortiGate-3 and FortiGate-4 with industrial protocol sensors.
B. Micro-segmentation can be achieved only by replacing FortiGate-3 and FortiGate-4 with a pair of FortiSwitch devices.
C. IT and OT networks are separated by segmentation.
D. FortiGate-3 and FortiGate-4 devices must be in a transparent mode.

Answer: A,C

Question No : 5

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

Question No : 6

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: C

Question No : 7

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: C,D,E

Question No : 8

Refer to the exhibit and analyze the output.

```
[PH_DEV_MON_NET_INTF_UTIL] : [eventSeverity] =PHL_INFO, [filename] =phPerfJob.cpp,
[lineNumber] =6646, [intfName]= Intel [R] PRO_100 MT Network
Connection, [intfAlias] =, [hostname] =WIN2K8DC, [hostIpAddr] = 192.168.69.6,
[pollIntv] =56, [recvBytes64] =
44273, [recvBitsPerSec] = 6324.714286, [inIntfUtil] = 0.000632, [sentBytes64] =
82014, [sentBitsPerSec] = 1171
6.285714, [outIntfUtil] = 0.001172, [recvPkts64] = 449, [sentPkts64] = 255,
[inIntfPktErr] = 0, [inIntfPktErrPct] = 0.000000, [outIntfPktErr] =0,
[outIntfPktErrPct] = 0.000000, [inIntfPktDiscarded] =0, [inIntfPktDiscardedPct] =
```

Which statement about the output is true?

A. This is a sample of a FortiAnalyzer system interface event log.

B. This is a sample of an SNMP temperature control event log.

C. This is a sample of a PAM event type.

D. This is a sample of FortiGate interface statistics.

Answer: C

Question No : 9

An OT administrator deployed many devices to secure the OT network. However, the SOC team is reporting that there are too many alerts, and that many of the alerts are false positive. The OT administrator would like to find a solution that eliminates repetitive tasks, improves efficiency, saves time, and saves resources.

Which products should the administrator deploy to address these issues and automate most of the manual tasks done by the SOC team?

A. FortiSIEM and FortiManager

B. FortiSandbox and FortiSIEM

C. FortiSOAR and FortiSIEM

D. A syslog server and FortiSIEM

Answer: C

Question No : 10

What are two benefits of a Nozomi integration with FortiNAC? (Choose two.)

A. Enhanced point of connection details
B. Direct VLAN assignment
C. Adapter consolidation for multi-adapter hosts
D. Importation and classification of hosts

Answer: A,D

Explanation: The two benefits of a Nozomi integration with FortiNAC are enhanced point of connection details and importation and classification of hosts. Enhanced point of connection details allows for the identification and separation of traffic from multiple points of connection, such as Wi-Fi, wired, cellular, and VPN. Importation and classification of hosts allows for the automated importing and classification of host and device information into FortiNAC. This allows for better visibility and control of the network.

Question No : 11

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.

Question No : 12