



- Expert Verified, Online, **Free**.



CERTIFICATION TEST

- CertificationTest.net - Cheap & Quality Resources With Best Support


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

Suggested Answer: AB

Community vote distribution

CD (100%)


 **azjlpang** 8 months, 3 weeks ago

Selected Answer: CD


- adapter consolidation for multi-adapter hosts
- Nozomi hosts will be imported and classified
Reference: FortiOS7.2_Study_Guide_page87
upvoted 1 times

 **John1216** 10 months ago

C. Adapter consolidation for multi-adapter hosts
D. Importation and classification of hosts
upvoted 1 times

 **mkd74** 11 months, 1 week ago

CD
pg 87 study guide
upvoted 1 times

 **ali_red** 1 year, 2 months ago

Selected Answer: CD

CD for sure
upvoted 1 times

 **Spippolo** 1 year, 4 months ago

Selected Answer: CD

Devices known to Nozomi can be imported and registered or classified automatically. The imported devices will be profiled based on information retrieved from the Nozomi product. Devices with multiple network adapters will have the devices consolidated under the single device in the FortiNAC.

upvoted 2 times

 **Niceone1** 1 year, 4 months ago

Selected Answer: CD

Correct Answer: CD
Explanation/Reference: Studyguide_page70
upvoted 1 times

 **cciesam** 1 year, 5 months ago


Selected Answer: CD

Ans: CD
upvoted 1 times

 **ekremyetis** 1 year, 9 months ago

Selected Answer: CD

CD is correct
upvoted 3 times

 **bigbug** 1 year, 9 months ago

Correct Answer: CD

Explanation/Reference:Studyguide_page70

upvoted 2 times

Which three criteria can a FortiGate device use to look for a matching firewall policy to process traffic? (Choose three.)

- A. Services defined in the firewall policy.
- B. Source defined as internet services in the firewall policy
- C. Lowest to highest policy ID number
- D. Destination defined as internet services in the firewall policy
- E. Highest to lowest priority defined in the firewall policy

Suggested Answer: ABD

  **John1216** 10 months ago

- A. Services defined in the firewall policy.
 - B. Source defined as internet services in the firewall policy
 - D. Destination defined as internet services in the firewall policy
- upvoted 2 times

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.

Suggested Answer: A

Community vote distribution

C (100%)


 **azjlpang** 8 months, 3 weeks ago

Selected Answer: C

All performance events have the prefix of PH_DEV_MON, which means a device monitoring event. FORTIOS7.2_StudyGuide_page231
upvoted 1 times

 **John1216** 10 months ago

C. This is a sample of a PAM event type.
upvoted 1 times

 **mkd74** 11 months, 1 week ago

C pg 230 and 231 study guide
upvoted 1 times

 **Spippolo** 1 year, 4 months ago

Selected Answer: C

C

All performance events have the prefix of PH DEV MON, which means a device monitoring event, or, put another way, an event derived from a performance monitoring poll.

upvoted 1 times

 **Niceone1** 1 year, 4 months ago


Selected Answer: C

This is a sample of a PAM event type.- SIEM see PAGE 209 study guide
upvoted 1 times

 **cciesam** 1 year, 5 months ago

Selected Answer: C

Ans: C
upvoted 1 times

 **Craygray** 1 year, 5 months ago

Selected Answer: C



Pg 209
upvoted 1 times

 **ilyak83** 1 year, 7 months ago

The answer is C.

Page 209 - OT_Security_6.4_Study_Guide-Online.pdf

upvoted 1 times

  **bigbug** 1 year, 9 months ago

C. PAM event PAGE 209

upvoted 3 times



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

Suggested Answer: ACD


Community vote distribution

ADE (100%)



  **azjlpang** 8 months, 3 weeks ago

Selected Answer: ADE

NGFW, FortiNAC and FortiSIEM can be used in an OT network to achieve asset identification and management. FortiOS7.2_Study_Guide_page18
upvoted 1 times

  **John1216** 10 months ago

- A. FortiNAC
 - D. FortiSIEM
 - E. FortiGate
- upvoted 1 times

  **mkd74** 11 months, 1 week ago

ADE, pg 18 study guide
upvoted 1 times

  **Spippolo** 1 year, 4 months ago


Selected Answer: ADE

pg. 16
upvoted 2 times

  **Niceone1** 1 year, 4 months ago

Selected Answer: ADE

PAGE 16
upvoted 1 times

  **cciesam** 1 year, 5 months ago

Selected Answer: ADE

Ans: ADE
upvoted 1 times

  **Net_Sec2** 1 year, 6 months ago

Selected Answer: ADE



Page 16 - OT_Security_6.4_Study_Guide-Online.pdf
upvoted 2 times

  **Jbeaulieu** 1 year, 6 months ago

Selected Answer: ADE

The answers are A,D and E.



Page 16 - OT_Security_6.4_Study_Guide-Online.pdf
upvoted 1 times

  **ilyak83** 1 year, 7 months ago

The answers are A,D and E.



Page 16 - OT_Security_6.4_Study_Guide-Online.pdf

upvoted 2 times

  **send2asela** 1 year, 8 months ago

ADE - Study guide Page 16

upvoted 2 times

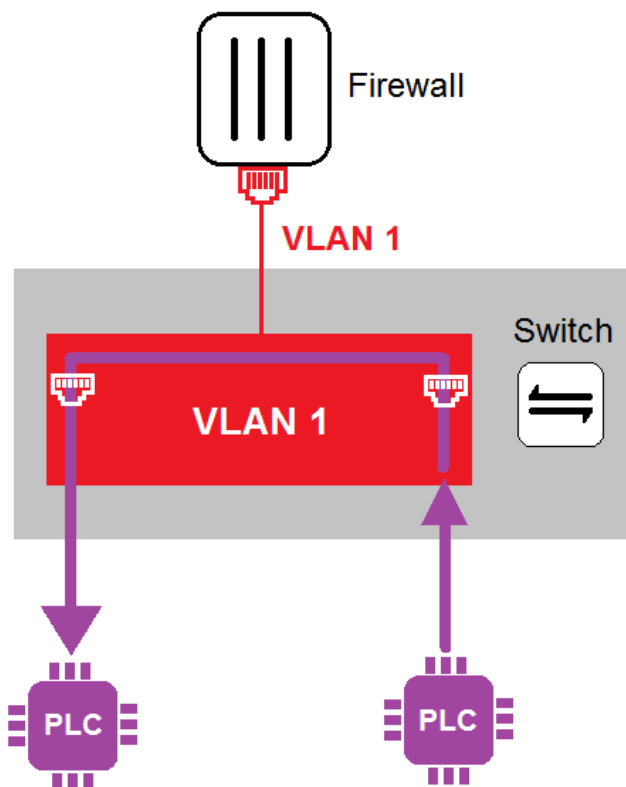
  **bigbug** 1 year, 9 months ago

Correct Answer: ACD

Reference:studyguid_page15&16

upvoted 1 times

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.

Suggested Answer: D

Community vote distribution

D (100%)

azjimpang 8 months, 3 weeks ago

Selected Answer: D

FortiOS7.2_Study_Guide_page150

upvoted 1 times

John1216 10 months ago

D. There is no micro-segmentation in this topology.

upvoted 1 times

Gain123 10 months, 1 week ago

Selected Answer: D

D is Correct

upvoted 1 times

ali_red 1 year, 2 months ago

D for sure



upvoted 1 times

Net_Sec2 1 year, 6 months ago

Selected Answer: D

Page 131 - OT_Security_6.4_Study_Guide-Online.pdf



upvoted 1 times

  **ilyak83** 1 year, 7 months ago

D.

Page 131 - OT_Security_6.4_Study_Guide-Online.pdf

upvoted 1 times

  **bigbug** 1 year, 9 months ago

Explanation/Reference:page_131

upvoted 1 times



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

Suggested Answer: A

Community vote distribution



A (100%)

  **azjlpang** 8 months, 3 weeks ago

Selected Answer: A

FortiNAC can use RADIUS on wired or wireless connection to gather visibility information and control access.

upvoted 1 times

  **John1216** 10 months ago

A. RADIUS

upvoted 1 times

  **cciesam** 1 year, 6 months ago

Selected Answer: A

Answer - A



upvoted 1 times

  **Net_Sec2** 1 year, 6 months ago

Selected Answer: A

Page 35 - OT_Security_6.4_Study_Guide-Online.pdf

upvoted 1 times

  **ilyak83** 1 year, 7 months ago

A.

Page 35 - OT_Security_6.4_Study_Guide-Online.pdf

upvoted 1 times

Which three common breach points can be found in a typical OT environment? (Choose three.)

- A. Global hat
- B. Hard hat
- C. VLAN exploits
- D. Black hat
- E. RTU exploits

Suggested Answer: CDE

Community vote distribution

BDE (100%)

🗳️ 👤 **bigbug** Highly Voted 1 year, 9 months ago

Correct Answer: BDE Section:

Explanation/Reference: studyguide_page179

upvoted 6 times

🗳️ 👤 **John1216** Most Recent 10 months ago

B. Hard hat

D. Black hat

E. RTU exploits

upvoted 1 times

🗳️ 👤 **ali_red** 1 year, 2 months ago

Selected Answer: BDE

BDE for sure

upvoted 1 times

🗳️ 👤 **Spippolo** 1 year, 4 months ago

Selected Answer: BDE

Breach points are everywhere in an OT environment, the most common breach points are: Outside threats from external hackers, Inside threat can be from industrial system operators, RTU security can be compromised, and the SCADA system is vulnerable to DoS and malicious control, Air gap can be breached in multiple locations allowing threats to propagate, DoS attack of industrial protocols RTU or HMI can be compromised through known exploits.

upvoted 3 times

🗳️ 👤 **cciesam** 1 year, 5 months ago

Selected Answer: BDE

Ans: BDE

upvoted 1 times












🗳️ 👤 **Net_Sec2** 1 year, 6 months ago

Selected Answer: BDE

Explanation/Reference: studyguide_page179

upvoted 3 times

Refer to the exhibit.

| Maint | Device | Type | Organization | Avail Status | Perf Status | Security Status |
|---|------------------|---------------------|--------------|---|---|---|
|  | FG240D3913800441 | Fortinet FortiOS | Super |  |  |  |
|  | SJ-QA-F-Lnx-CHK | Checkpoint FireWall | Super |  |  |  |
|  | FAPS321C-default | Fortinet FortiAP | Super | |  |  |

You are navigating through FortiSIEM in an OT network.


How do you view information presented in the exhibit and what does the FortiGate device security status tell you?

- A. In the PCI logging dashboard and there are one or more high-severity security incidents for the FortiGate device.
- B. In the summary dashboard and there are one or more high-severity security incidents for the FortiGate device.
- C. In the widget dashboard and there are one or more high-severity incidents for the FortiGate device.
- D. In the business service dashboard and there are one or more high-severity security incidents for the FortiGate device.

Suggested Answer: B

Community vote distribution

B (100%)

 **azjimpang** 8 months, 2 weeks ago

Selected Answer: B

This one is a summary dashboard

Study Guide_NSE7 OT 7.2 p258

upvoted 1 times

 **John1216** 10 months ago

B. In the summary dashboard and there are one or more high-severity security incidents for the FortiGate device.


upvoted 1 times

 **Spippolo** 1 year, 4 months ago

Selected Answer: B

Pag. 259 – Study Guide | NSE7 OT 6.4

upvoted 1 times

 **bigbug** 1 year, 9 months ago

Explanation/Reference:studyguide_page259

upvoted 2 times

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

Suggested Answer: AB

Community vote distribution

AD (100%)

🗳️ 👤 **azjlpang** 8 months, 2 weeks ago

Selected Answer: AD

Local Authentication, remote authentication and 2FA are called active authentication.

Study Guide | NSE7 OT 7.2 page 80

upvoted 1 times

🗳️ 👤 **John1216** 10 months ago

A. Two-factor authentication on FortiAuthenticator & D. Local authentication on FortiGate

upvoted 1 times

🗳️ 👤 **ollo79** 1 year ago

Selected Answer: AD

AD pag97 - 7.2

upvoted 1 times

🗳️ 👤 **ali_red** 1 year, 2 months ago

Selected Answer: AD

AD for sure

upvoted 1 times

🗳️ 👤 **Spippolo** 1 year, 4 months ago

Selected Answer: AD

Pag. 80 – Study Guide | NSE7 OT 6.4

upvoted 1 times

🗳️ 👤 **cciesam** 1 year, 5 months ago

Selected Answer: AD

Ans: AD

upvoted 2 times

🗳️ 👤 **cubcub319** 1 year, 9 months ago

Selected Answer: AD

role based and fsso are passive

upvoted 4 times

🗳️ 👤 **bigbug** 1 year, 9 months ago

Explanation/Reference: studyguide_page79&80

upvoted 1 times

Refer to the exhibit.

| Router/Switch Image Distribution | | | | | |
|---|--------------------|-------------------|-----------------------|---|-------|
| <div> <div>Active Rules</div> <div>Windows Installed Patches</div> <div>Router/Switch Image Distribution</div> </div> | | | | | |
| <div> <div>Back</div> <div>Export</div> <div>1/1</div> <div>3</div> </div> | | | | | |
| 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

Suggested Answer: A

Community vote distribution

A (100%)

 **azjlpang** 8 months, 2 weeks ago

Selected Answer: A

A FortiSIEM CMDB report

OT Security 7.2 Study Guide - page 255
upvoted 1 times

 **John1216** 10 months ago

A. A FortiSIEM CMDB report
upvoted 1 times

 **Spippolo** 1 year, 4 months ago

Selected Answer: A

One use case for CMDB reports is device inventories. In FortiSIEM, you can run a device inventory report to look at image files on all routers, switches, and firewalls to identify vulnerable firmware versions.
upvoted 1 times

 **Niceone1** 1 year, 4 months ago

Selected Answer: A

Verified on SIEM console
upvoted 1 times

 **Net_Sec2** 1 year, 6 months ago

Selected Answer: A

Explanation/Reference: studyguide_page253
upvoted 2 times

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

Suggested Answer: C

Community vote distribution

C (100%)

🗳️ 👤 **azjimpang** 8 months, 2 weeks ago

Selected Answer: C

FortiSOAR and FortiSIEM

upvoted 1 times

🗳️ 👤 **John1216** 10 months ago

C. FortiSOAR and FortiSIEM

upvoted 1 times

🗳️ 👤 **Spippolo** 1 year, 4 months ago

Selected Answer: C

For exclusion C.

FortiSOAR is a product that can be used to automate the response to reported incident.

upvoted 1 times

🗳️ 👤 **bigbug** 1 year, 9 months ago

Explanation/Reference:Studyguide_FortiSOAR_page20

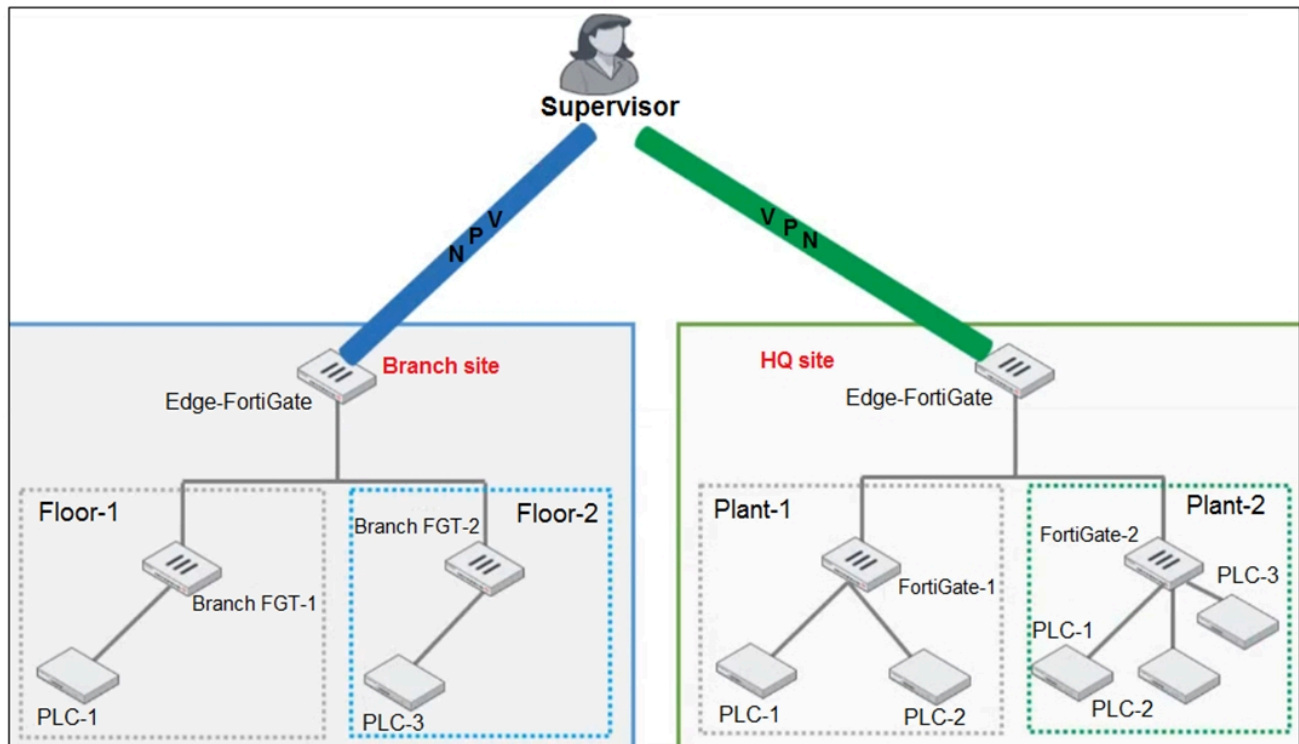
upvoted 1 times

🗳️ 👤 **bigbug** 1 year, 9 months ago

Explanation/Reference:studyguide_page255

upvoted 1 times

Refer to the exhibit.



You need to configure VPN user access for supervisors at the branch 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.

Suggested Answer: A

Community vote distribution

A (100%)

azjimpang 8 months, 2 weeks ago

Selected Answer: A

FortiAuthenticator can support multiple FortiGate devices or other third-party vendor devices. With FortiAuthenticator, one FortiToken can be used to authenticate to multiple systems

OT Security 7.2 Study Guide Page 92

upvoted 1 times

John1216 10 months ago

A. You must use a FortiAuthenticator.

upvoted 1 times



Spippolo 1 year, 4 months ago

Selected Answer: A

A.

FortiAuthenticator can support multiple FortiGate devices or other third-party vendor devices. With FortiAuthenticator, one FortiToken can be used to authenticate to multiple systems.

upvoted 1 times

  **bigbug** 1 year, 9 months ago

Explanation/Reference:page92

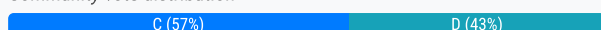
upvoted 1 times

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.

Suggested Answer: D

Community vote distribution



GCISystemIntegrator 6 months, 3 weeks ago

Selected Answer: D

only with the command in D option permit to have passive and active auth.
with FSSO no user prompt regardless order of any firewall policy.
upvoted 1 times

azjimpang 1 year, 2 months ago

Selected Answer: C

C. Configure a firewall policy with FSSO users and place it on the top of list of firewall policies.
upvoted 1 times

John1216 1 year, 4 months ago

D. Under config user settings configure set auth-on-demand implicit.
upvoted 1 times

ollo79 1 year, 6 months ago

C, auth-on-demand implicit is default
upvoted 2 times

ali_red 1 year, 8 months ago

Selected Answer: C

C for sure
upvoted 1 times

Spippolo 1 year, 10 months ago

Selected Answer: C

C.

When you enable authentication, all the systems will have to authenticated before traffic is placed on egress interface. Alternatively, on the CLI only, you can change the auth-on-demand option to always.
upvoted 1 times

cciesam 1 year, 11 months ago

Selected Answer: C

Ans: C
upvoted 1 times

Net_Sec2 2 years ago

Selected Answer: D

Explanation/Reference: studyguide_page88
upvoted 2 times

bigbug 2 years, 3 months ago

C Explanation/Reference: studyguide_page88
upvoted 4 times

An OT network architect needs to secure control area zones with a single network access policy to provision devices to any number of different networks.

On which device can this be accomplished?

- A. FortiGate
- B. FortiEDR
- C. FortiSwitch
- D. FortiNAC

Suggested Answer: D

Community vote distribution

D (100%)

🗳️ 👤 **myrmidon3** 1 year ago

OT Security 7.2 Study Guide p 124.

Network Access Policies are used to dynamically provision access to connecting endpoints, based on the matched user/host profiles associated with the network access configuration.

Answer is D, FortiNAC.

upvoted 1 times

🗳️ 👤 **azjlpang** 1 year, 2 months ago

D. FortiNAC

upvoted 1 times

🗳️ 👤 **John1216** 1 year, 4 months ago

D. FortiNAC

upvoted 1 times

🗳️ 👤 **ali_red** 1 year, 8 months ago

Selected Answer: D

D for sure

upvoted 1 times

🗳️ 👤 **Spippolo** 1 year, 10 months ago

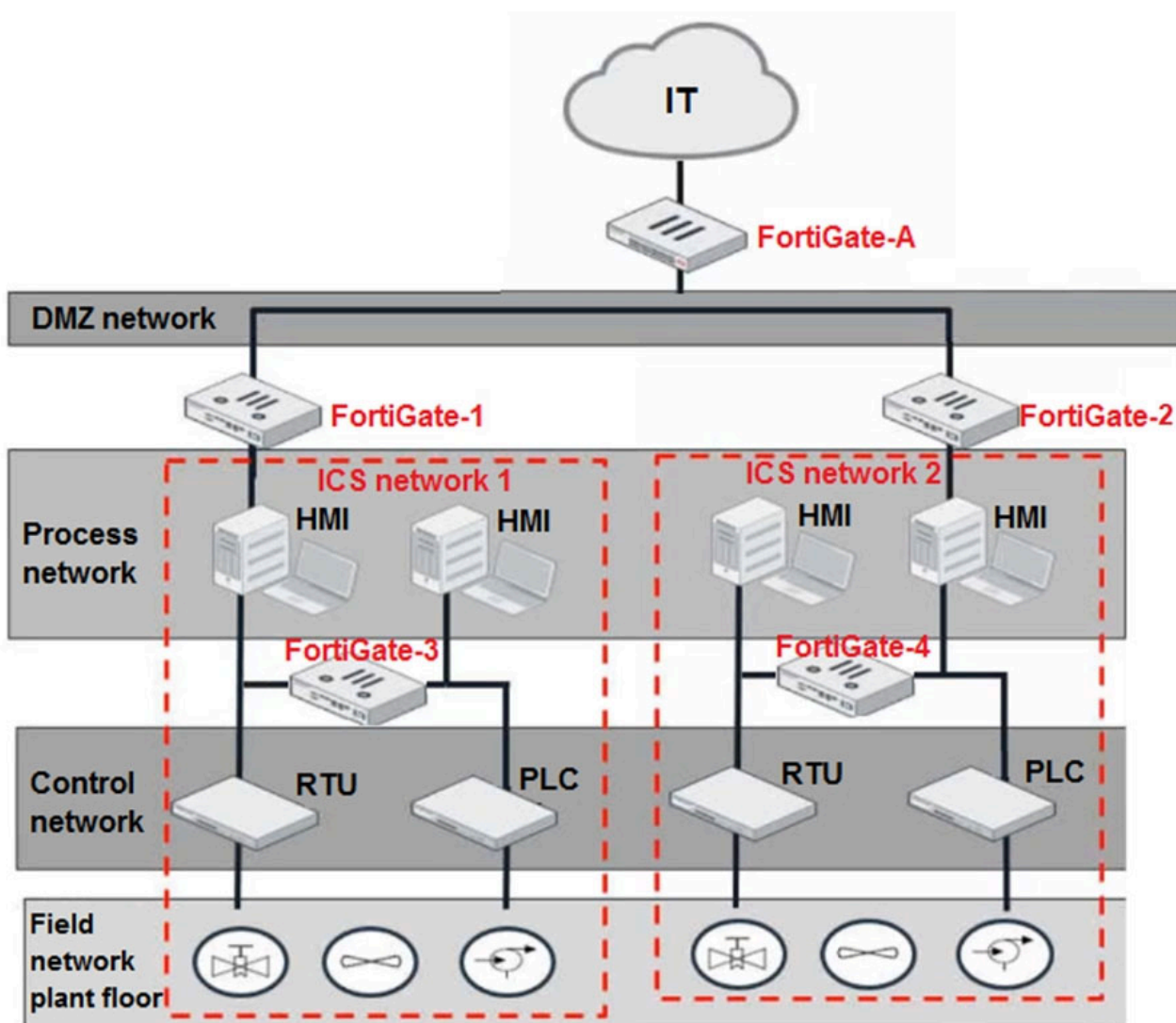
Selected Answer: D

Should be D.

Network access policies are used to dynamically provision access to connecting endpoints, based on the matched user/host profiles associated with the network access configurations.

upvoted 1 times

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.

Suggested Answer: CD

Community vote distribution

AC (100%)

azjimpang 8 months, 2 weeks ago

1A. Firewall policies should be configured on FortiGate-3 and FortiGate-4 with industrial protocol sensor

2A. and OT ntwork are separated ny segmentation

upvoted 1 times

John1216 10 months ago

A. Firewall policies should be configured on FortiGate-3 and FortiGate-4 with industrial protocol sensors. & C. IT and OT networks are separated by segmentation.

upvoted 2 times

cciesam 1 year, 5 months ago

Selected Answer: AC

Ans: AC



upvoted 2 times

  **Net_Sec2** 1 year, 6 months ago

Selected Answer: AC

Explanation/Reference:studyguide_page181

upvoted 2 times

  **bigbug** 1 year, 9 months ago

A and C

Explanation/Reference:studyguide_page181

upvoted 2 times