



Fortinet

Exam Questions NSE7_OTS-6.4

Fortinet NSE 7 - OT Security 6.4

NEW QUESTION 1

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

Answer: D

NEW QUESTION 2

An OT administrator has configured FSSO and local firewall authentication. A user who is part of a user group is not prompted from credentials during authentication. What is a possible reason?

- A. FortiGate determined the user by passive authentication
- B. The user was determined by Security Fabric
- C. Two-factor authentication is not configured with RADIUS authentication method
- D. FortiNAC determined the user by DHCP fingerprint method

Answer: D

NEW QUESTION 3

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

Answer: CDE

NEW QUESTION 4

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 5

Refer to the exhibit.

Active Rules x

Windows Installed Patches x

Router/Switch Image Distribution x

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.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?

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

Answer: A

NEW QUESTION 6

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 7

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 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: A

NEW QUESTION 9

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 10

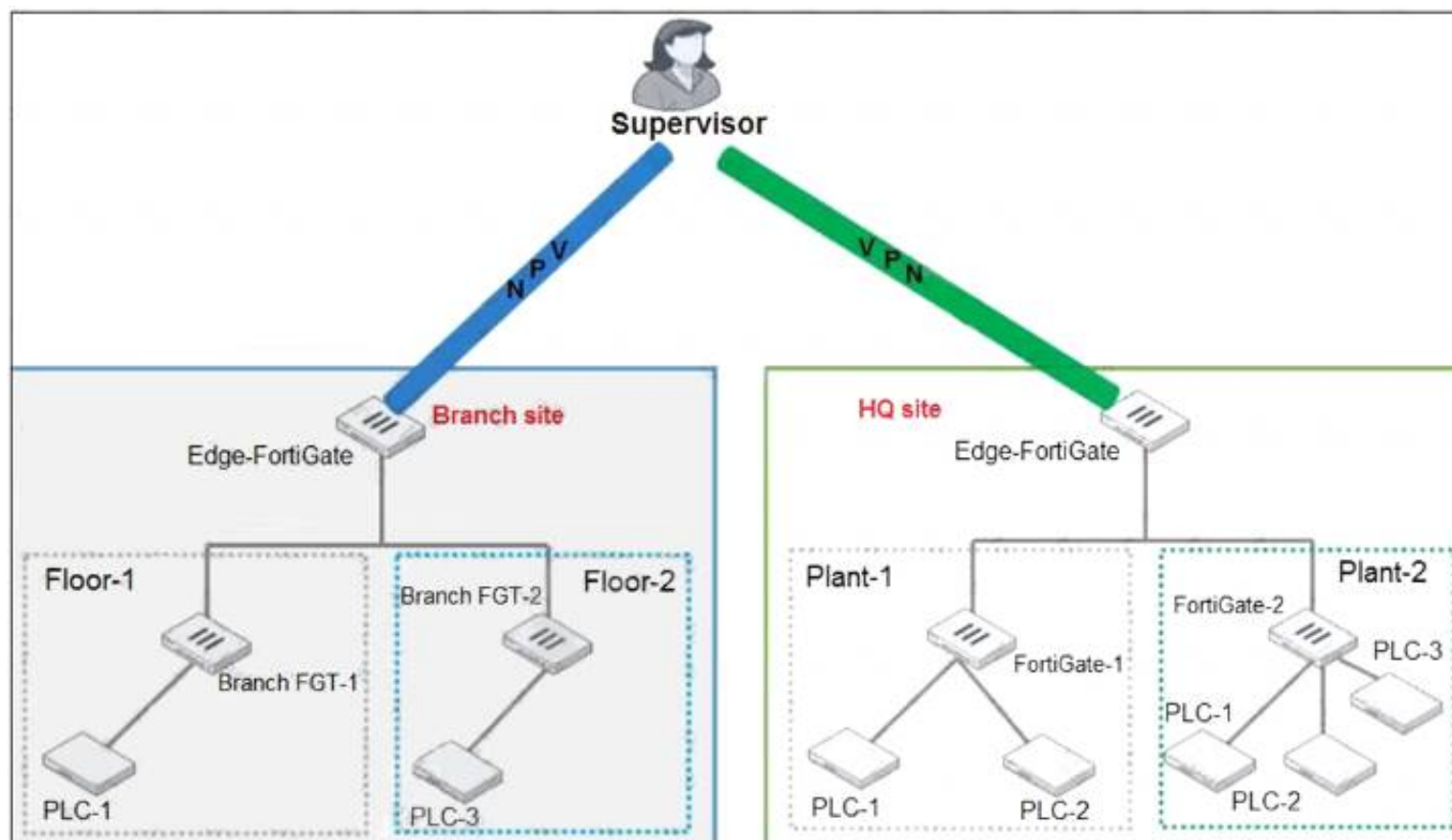
Which three methods of communication are used by FortiNAC to gather visibility information? (Choose three.)

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

Answer: ACD

NEW QUESTION 10

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 15

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 19

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 21

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

NSE7_OTS-6.4 Practice Exam Features:

- * NSE7_OTS-6.4 Questions and Answers Updated Frequently
- * NSE7_OTS-6.4 Practice Questions Verified by Expert Senior Certified Staff
- * NSE7_OTS-6.4 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * NSE7_OTS-6.4 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The NSE7_OTS-6.4 Practice Test Here](#)