Exam Questions NSE7_OTS-7.2

Fortinet NSE 7 - OT Security 7.2

https://www.2passeasy.com/dumps/NSE7_OTS-7.2/

NEW QUESTION 1
To increase security protection in an OT network, how does application control on ForliGate detect industrial traffic?

A. By inspecting software and software-based vulnerabilities
B. By inspecting applications only on nonprotected traffic
C. By inspecting applications with more granularity by inspecting subapplication traffic
D. By inspecting protocols used in the application traffic

Answer: B

NEW QUESTION 2
Which two frameworks are common to secure ICS industrial processes, including SCADA and DCS? (Choose two.)

A. Modbus
B. NIST Cybersecurity
C. IEC 62443
D. IEC104

Answer: CD

NEW QUESTION 3
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 4
The OT network analyst runs different level of reports to quickly explore threats that exploit the network. Such reports can be run on all routers, switches, and firewalls. Which FortiSIEM reporting method helps to identify these type of exploits of image firmware files?

A. CMDB reports
B. Threat hunting reports
C. Compliance reports
D. OT/loT reports

Answer: B

NEW 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?

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

Explanation:
This way, FortiSIEM can discover and monitor everything attached to the remote network and provide security visibility to the corporate network

NEW QUESTION 6
An OT network consists of multiple FortiGate devices. The edge FortiGate device is deployed as the secure gateway and is only allowing remote operators to access the ICS networks on site.
Management hires a third-party company to conduct health and safety on site. The third- party company must have outbound access to external resources.
As the OT network administrator, what is the best scenario to provide external access to the third-party company while continuing to secure the ICS networks?

A. Configure outbound security policies with limited active authentication users of the third- party company.
B. Create VPN tunnels between downstream FortiGate devices and the edge FortiGate to protect ICS network traffic.
C. Split the edge FortiGate device into multiple logical devices to allocate an independent VDOM for the third-party company.
D. Implement an additional firewall using an additional upstream link to the internet.

Answer: C

NEW QUESTION 7
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

NEW QUESTION 8
What are two critical tasks the OT network auditors must perform during OT network risk assessment and management? (Choose two.)

A. Planning a threat hunting strategy
B. Implementing strategies to automatically bring PLCs offline
C. Creating disaster recovery plans to switch operations to a backup plant
D. Evaluating what can go wrong before it happens

Answer: BC

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 type of attack posed by skilled and malicious users of security level 4 (SL 4) of IEC 62443 is designed to defend against intentional attacks?

A. Users with access to moderate resources
B. Users with low access to resources
C. Users with unintentional operator error
D. Users with substantial resources

Answer: C

NEW QUESTION 10
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

Answer: ADE

Explanation:
The three criteria that a FortiGate device can use to look for a matching firewall policy to process traffic are:
* A. Services defined in the firewall policy - FortiGate devices can match firewall policies based on the services defined in the policy, such as HTTP, FTP, or DNS.
* D. Destination defined as internet services in the firewall policy - FortiGate devices can also match firewall policies based on the destination of the traffic, including destination IP address, interface, or internet services.
* E. Highest to lowest priority defined in the firewall policy - FortiGate devices can prioritize firewall policies based on the priority defined in the policy. The device will process traffic against the policy with the highest priority first and move down the list until it finds a matching policy.
Reference:
Fortinet NSE 7 - Enterprise Firewall 6.4 Study Guide, Chapter 4: Policy Implementation, page 4-18.

NEW QUESTION 14
As an OT network administrator, you are managing three FortiGate devices that each protect different levels on the Purdue model. To increase traffic visibility, you are required to implement additional security measures to detect exploits that affect PLCs.
Which security sensor must implement to detect these types of industrial exploits?

A. Intrusion prevention system (IPS)
B. Deep packet inspection (DPI)
C. Antivirus inspection
D. Application control

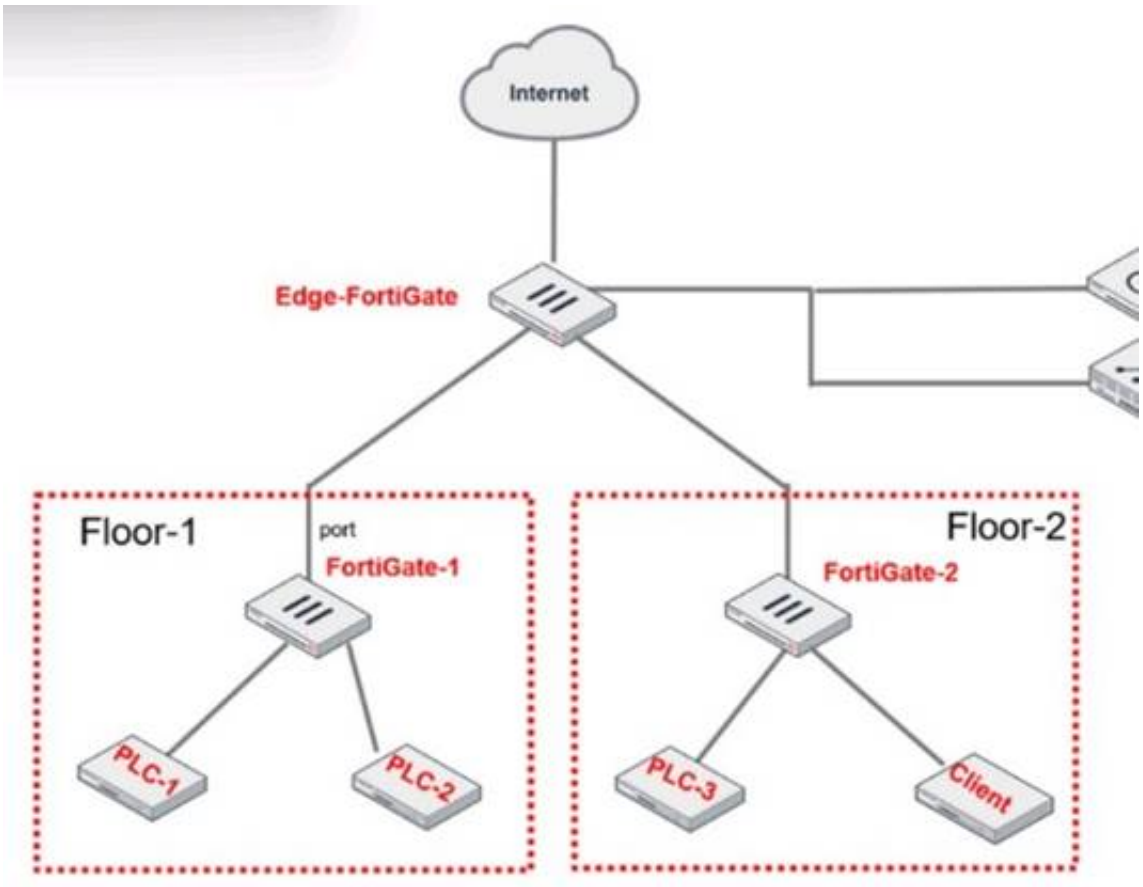
Answer: B

NEW QUESTION 18
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: A

NEW QUESTION 22
Refer to the exhibit.

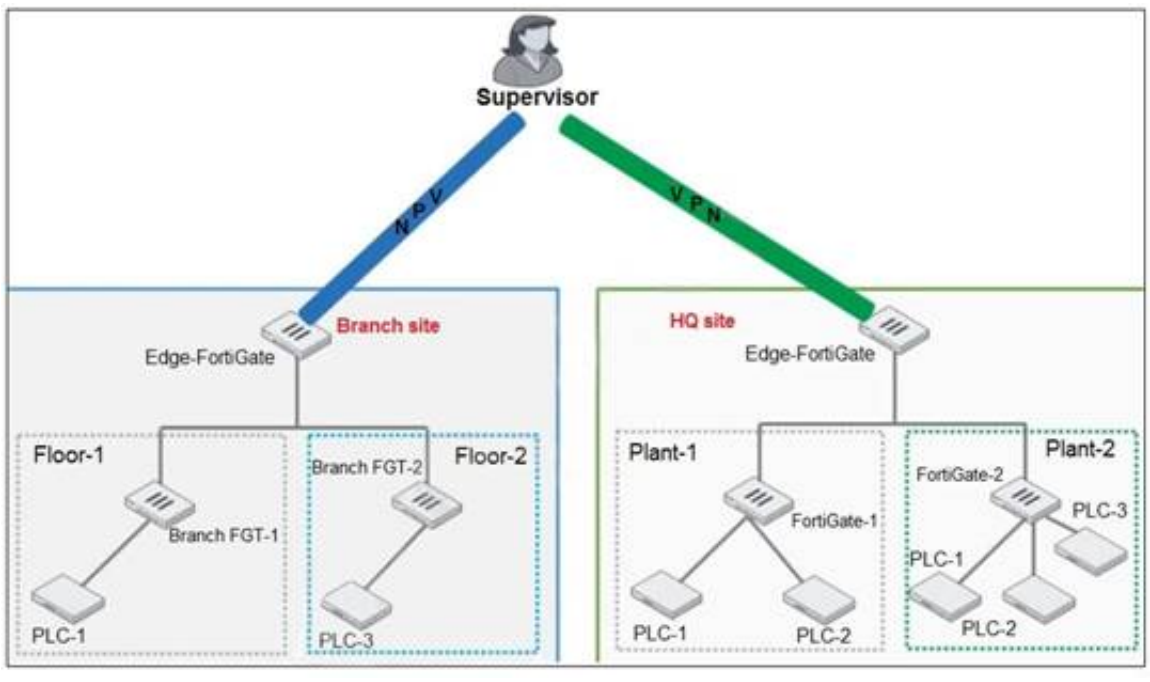


PLC-3 and CLIENT can send traffic to PLC-1 and PLC-2. FGT-2 has only one software switch (SSW-1) connecting both PLC-3 and CLIENT. PLC-3 and CLIENT can send traffic to each other at the Layer 2 level.
What must the OT admin do to prevent Layer 2-level communication between PLC-3 and CLIENT?

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

Answer: AB

NEW QUESTION 23
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 25
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

Explanation:
https://docs.fortinet.com/document/fortinac/9.2.0/administration-guide/15797/user-host-profiles

NEW QUESTION 26
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: A

Explanation:
An OT network architect can accomplish the goal of securing control area zones with a single network access policy to provision devices to any number of different networks on a FortiGate device.

NEW QUESTION 31
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: AB

Explanation:
Ref: https://docs.fortinet.com/document/fortianalyzer/7.0.0/administration-guide/268882/fortisoc

NEW QUESTION 32
Which two statements are true when you deploy FortiGate as an offline IDS? (Choose two.)

A. FortiGate receives traffic from configured port mirroring.
B. Network traffic goes through FortiGate.
C. FortiGate acts as network sensor.
D. Network attacks can be detected and blocked.

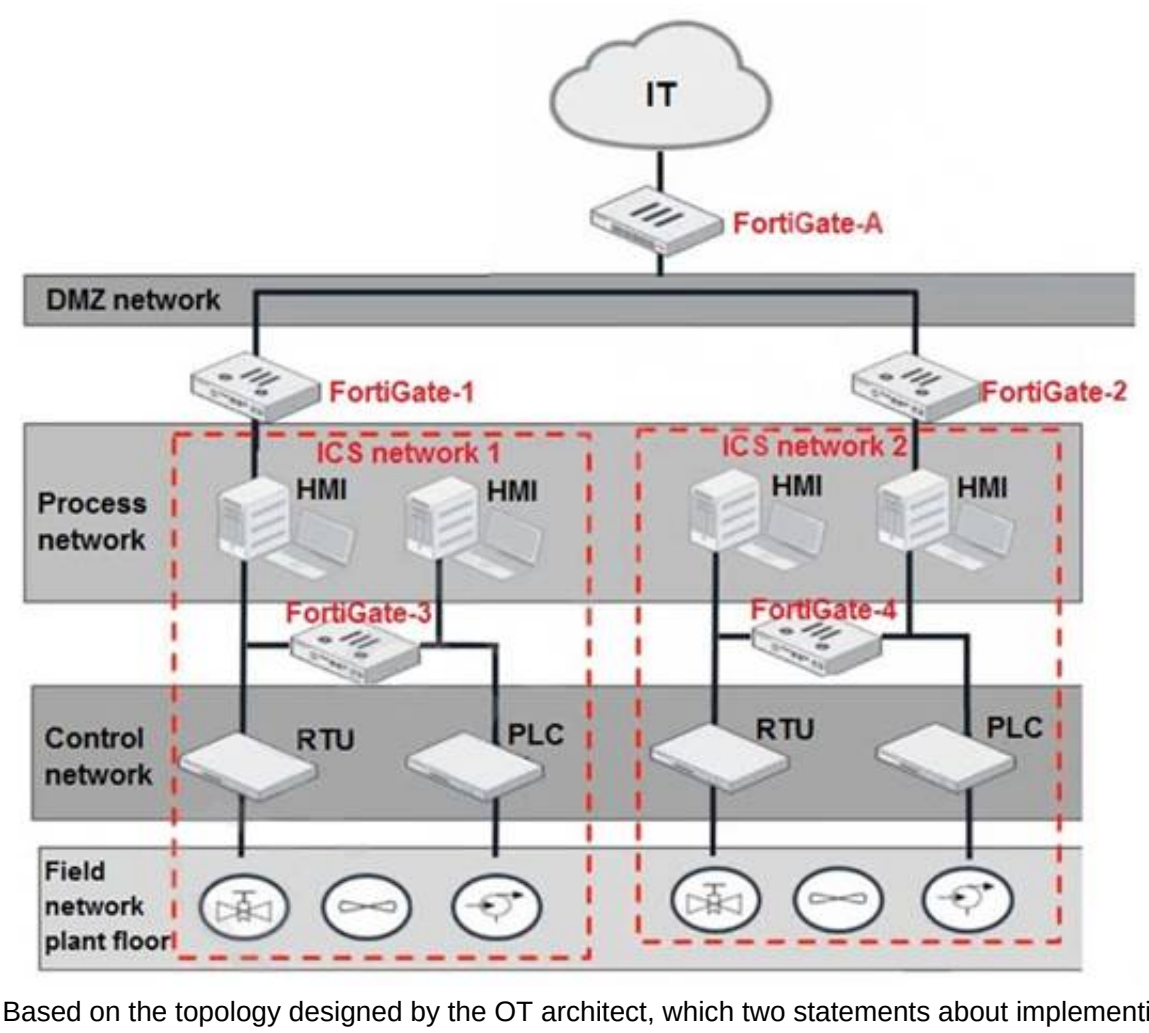
Answer: BC

NEW QUESTION 33
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 34
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: AC

NEW QUESTION 35
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.

NEW QUESTION 36
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

NEW QUESTION 38
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.

Answer: B

NEW QUESTION 42
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual NSE7_OTS-7.2 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the NSE7_OTS-7.2 Product From:

https://www.2passeasy.com/dumps/NSE7_OTS-7.2/

Money Back Guarantee

NSE7_OTS-7.2 Practice Exam Features:

* NSE7_OTS-7.2 Questions and Answers Updated Frequently

* NSE7_OTS-7.2 Practice Questions Verified by Expert Senior Certified Staff

* NSE7_OTS-7.2 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* NSE7_OTS-7.2 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year