



Vendor: Fortinet

Exam Code: NSE7_OTC-7.2

Exam Name: Fortinet NSE 7 - OT Security 7.2

Version: DEMO

QUESTION 1

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

QUESTION 2

An OT architect has deployed a Layer 2 switch in the OT network at Level 1 the Purdue model-process control. The purpose of the Layer 2 switch is to segment traffic between PLC1 and PLC2 with two VLANs. All the traffic between PLC1 and PLC2 must first flow through the Layer 2 switch and then through the FortiGate device in the Level 2 supervisory control network. What statement about the traffic between PLC1 and PLC2 is true?

- A. The Layer 2 switch rewrites VLAN tags before sending traffic to the FortiGate device.
- B. The Layer 2 switches routes any traffic to the FortiGate device through an Ethernet link.
- C. PLC1 and PLC2 traffic must flow through the Layer-2 switch trunk link to the FortiGate device.
- D. In order to communicate, PLC1 must be in the same VLAN as PLC2.

Answer: C

Explanation:

The statement that is true about the traffic between PLC1 and PLC2 is that PLC1 and PLC2 traffic must flow through the Layer-2 switch trunk link to the FortiGate device.

QUESTION 3

An OT administrator is defining an incident notification policy using FortiSIEM and would like to configure the system with a notification policy. If an incident occurs, the administrator would like to be able to intervene and block an IP address or disable a user in Active Directory from FortiSIEM. Which step must the administrator take to achieve this task?

- A. Configure a fabric connector with a notification policy on FortiSIEM to connect with FortiGate.
- B. Create a notification policy and define a script/remediation on FortiSIEM.
- C. Define a script/remediation on FortiManager and enable a notification rule on FortiSIEM.
- D. Deploy a mitigation script on Active Directory and create a notification policy on FortiSIEM.

Answer: B

Explanation:

<https://fusecommunity.fortinet.com/blogs/silviu/2022/04/12/fortisiempublishingscript>

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

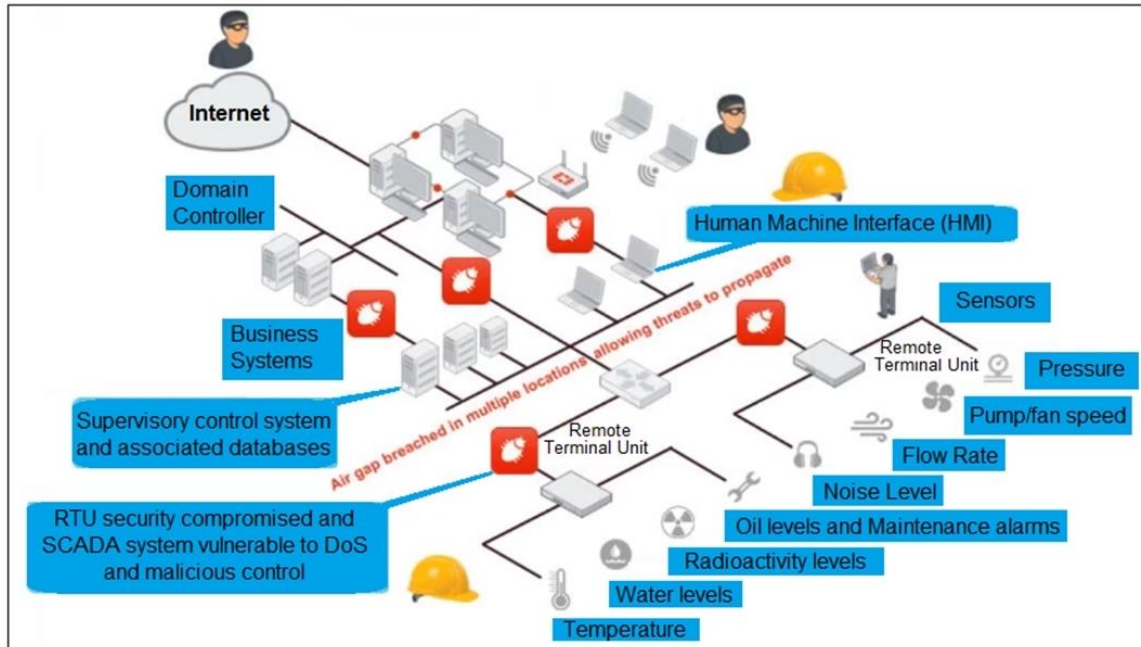
Answer: ADE

Explanation:

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

QUESTION 5

Refer to the exhibit, which shows a non-protected OT environment.



An administrator needs to implement proper protection on the OT network. Which three steps should an administrator take to protect the OT network? (Choose three.)

- A. Deploy an edge FortiGate between the internet and an OT network as a one-arm sniffer.
- B. Deploy a FortiGate device within each ICS network.
- C. Configure firewall policies with web filter to protect the different ICS networks.
- D. Configure firewall policies with industrial protocol sensors
- E. Use segmentation

Answer: ACD

QUESTION 6

An OT administrator has configured FSSO and local firewall authentication. A user who is part of a user group is not prompted for 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

QUESTION 7

Refer to the exhibit. Given the configurations on the FortiGate, which statement is true?

```
config system interface
  edit VLAN101_dmz
    set forward-domain 101
next
  edit VLAN101_internal
    set forward-domain 101
end
```

- 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

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

- ★ More than **99,900** Satisfied Customers Worldwide.
- ★ Average **99.9%** Success Rate.
- ★ **Free Update** to match latest and real exam scenarios.
- ★ **Instant Download** Access! No Setup required.
- ★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.
- ★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.
- ★ **100%** Guaranteed Success or **100%** Money Back Guarantee.
- ★ **Fast**, helpful support **24x7**.



View list of all certification exams: <http://www.lead2pass.com/all-products.html>



Microsoft



ORACLE



CITRIX



JUNIPER
NETWORKS



EMC²
where information lives

10% Discount Coupon Code: ASTR14