

DUMPSQUEEN

Fortinet NSE 7 - OT Security 6.4

Fortinet NSE7 OTS-6.4

Version Demo

Total Demo Questions: 5

Total Premium Questions: 35

Buy Premium PDF

<https://dumpsqueen.com>

support@dumpsqueen.com

dumpsqueen.com

QUESTION NO: 1

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: 2

As an OT administrator, it is important to understand how industrial protocols work in an OT network.

Which communication method is used by the Modbus protocol?

- A. It uses OSI Layer 2 and the primary device sends data based on request from secondary device.
- B. It uses OSI Layer 2 and both the primary/secondary devices always send data during the communication.
- C. It uses OSI Layer 2 and both the primary/secondary devices send data based on a matching token ring.
- D. It uses OSI Layer 2 and the secondary device sends data based on request from primary device.

ANSWER: D

QUESTION NO: 3

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 NO: 4

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: 5

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: B D E