PassQueen
a.k.a dumpsqueen.com

Fortinet NSE 7 - OT Security 7.2

Fortinet NSE7_OTS-7.2

Version Demo

Total Demo Questions: 2

Total Premium Questions: 23

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, OT Security	1
Topic 2, FortiGate	20
Topic 3, FortiNAC	1
Topic 4, FortiAnalyzer	1
Total	23

QUESTION NO: 1

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:

Configure a firewall policy with FSSO users and place it on the top of list of firewall policies. FortiGate evaluates firewall policies in sequence, from the top of the policy list downward. Placing the policy that references the FSSO user group first lets FortiGate use the identity learned passively through FSSO whenever an authenticated user's IP address and group membership are already present in the FSSO information.

If a user has not been identified through the passive FSSO process, that user does not satisfy the FSSO identity requirement for this first policy. Traffic can then be evaluated against a subsequent policy that uses the LDAP user group and requires interactive authentication. This policy sequence delivers the intended behavior: transparent access for users whose identities are available from FSSO, followed by an active authentication challenge only when passive identity detection has not succeeded.

FSSO is Fortinet's mechanism for collecting user logon and group information from directory and logon sources so that FortiGate can apply identity-based policy without initially prompting the user. See the FortiGate 7.2 Administration Guide and Fortinet's Fortinet Single Sign-On overview.

QUESTION NO: 2

An OT administrator has applied an application control profile to a firewall policy that permits HTTPS access from a maintenance subnet to a vendor portal. The profile is intended to block file uploads, but FortiGate identifies only generic SSL traffic and does not detect the web application.

What should the administrator do to allow application control to inspect the HTTPS application traffic?

A. Apply a deep SSL inspection profile to the firewall policy.

B. Apply a certificate inspection profile to the firewall policy.

C. Move the firewall policy below the implicit deny policy.

D. Configure FSSO authentication for the maintenance subnet.

ANSWER: A

Explanation:

Apply a deep SSL inspection profile to the policy, provided that the managed endpoints trust the FortiGate inspection certificate. Deep inspection decrypts supported SSL/TLS traffic so that FortiGate can identify the application and inspect its content.

Certificate inspection validates and examines certificate information but does not provide the decrypted payload required for full application and content inspection. Changing the policy order or enabling a different authentication method does not make encrypted application content visible.