DUMPSBOSS.

FCPFortiAuthenticator 6.5 Administrator

Fortinet FCP_FAC_AD-6.5

Version Demo

Total Demo Questions: 4

Total Premium Questions: 41

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

Topic Break Down

Topic	No. of Questions
Topic 1, Initial Configuration	1
Topic 2, Authentication	12
Topic 3, User Management	4
Topic 4, Two-Factor Authentication	4
Topic 5, Certificate Management	13
Topic 6, Fortinet Single Sign-On	5
Topic 7, High Availability	2
Total	41

QUESTION NO: 1

You have implemented two-factor authentication to enhance security to sensitive enterprise systems.

How could you bypass the need for two-factor authentication for users accessing form specific secured networks?

A. Enable Adaptive Authentication in the portal policy.

B. Specify the appropriate RADIUS clients in the authentication policy.

C. Create an admin realm in the authentication policy.

D. Enable the Resolve user geolocation from their IP address option in the authentication policy

ANSWER: A

Explanation:

Enable Adaptive Authentication in the portal policy. is correct because FortiAuthenticator Adaptive Authentication evaluates contextual information associated with a portal login and applies the appropriate authentication requirements. A portal policy can use a trusted network condition, such as the source IP address or network from which the user connects, to identify access originating from a secured internal network. When the defined condition is met, the policy can permit the user to authenticate without requiring the additional second-factor challenge. For connections that do not meet the trusted-network context, the policy can continue to enforce two-factor authentication, preserving stronger protection for remote or otherwise untrusted access. This provides a risk- and context-aware authentication experience rather than applying an identical MFA requirement to every login regardless of where it originates. The configuration belongs in the portal policy because that policy governs the authentication behavior for users accessing the relevant portal and can apply Adaptive Authentication rules during that access flow. Fortinet documents portal authentication and policy configuration in the FortiAuthenticator 6.5 Administration Guide. Fortinet's product documentation portal is also available at FortiAuthenticator documentation.

QUESTION NO: 2

A FortiAuthenticator local CA is used as the root CA for an internal certificate hierarchy.

Which two statements about the root CA private key are true? (Choose two.)

A. It must be protected from unauthorized access.

B. It can be used to sign subordinate CA certificates.

C. It is distributed to clients as part of the root CA certificate.

D. It is included in the CA certificate revocation list.

ANSWER: A B

Explanation:

The root CA private key must be protected from unauthorized access because possession of it would allow an attacker to create certificates that appear to have been issued by the trusted root CA. This would compromise the trust of the entire hierarchy.

The root CA private key can be used to sign subordinate CA certificates is also correct. A root CA establishes trust for subordinate issuing CAs by signing their certificates.

The root CA private key is not distributed in certificates. Certificates contain public keys, and distributing the private key to clients or including it in a CRL would defeat the security of the PKI.

QUESTION NO: 3

A network administrator is using FortiAuthenticator as their RADIUS server for wired and wireless network access. The administrator wants to pass the users' group information back to the RADIUS clients when the users authenticate.

How does FortiAuthenticator accomplish this?

A. RADIUS attributes

B. RADIUS accounting

C. Syslog messages

D. REST API

ANSWER: A

Explanation:

RADIUS attributes are the mechanism FortiAuthenticator uses to return authorization-related information to a RADIUS client as part of a successful authentication response. When a user authenticates, FortiAuthenticator can evaluate the user's group membership and include configured response attributes in the RADIUS Access-Accept message. These attributes provide the network access device—such as a wireless controller, switch, firewall, or VPN gateway—with information it can use to apply its own authorization policy. For example, a client can use a returned group-related attribute to assign a role, VLAN, access-control policy, or other permission set appropriate to that user's group.

This approach keeps authentication and identity-group lookup centralized on FortiAuthenticator while allowing each RADIUS client to enforce access according to the attributes it receives. In FortiAuthenticator, RADIUS policies can match users or groups and apply the required RADIUS attribute values in the response. The exact attribute used depends on the consuming device and its RADIUS integration requirements, including support for standard or vendor-specific attributes. Fortinet documents RADIUS policy configuration and attribute assignment in the FortiAuthenticator Administration Guide: FortiAuthenticator 6.5 Administration Guide. The underlying RADIUS Access-Accept attribute model is defined by the IETF in RFC 2865.

QUESTION NO: 4

A RADIUS client sends a user name and password to FortiAuthenticator. The password is valid, but the applicable RADIUS policy requires a FortiToken OTP. FortiAuthenticator returns an Access-Challenge.

Which two conditions must be met for the authentication to complete successfully? (Choose two.)

A. The RADIUS client must support RADIUS Access-Challenge processing.

B. The RADIUS client must return the OTP response in a subsequent authentication request.

C. The RADIUS policy must return an Access-Accept before the OTP is validated.

D. The RADIUS client must send an accounting Start message containing the OTP.

ANSWER: A B

Explanation:

The RADIUS client must support Access-Challenge processing and must prompt for, or otherwise obtain, the additional OTP. It must then return the user response to FortiAuthenticator in a subsequent RADIUS authentication request so that FortiAuthenticator can validate the second factor.

Changing the policy to return Access-Accept would bypass the required second factor rather than complete two-factor authentication. RADIUS accounting records session activity and is not used to carry the OTP challenge response.