DUMPSBOSS.

Fortinet NSE 6 - FortiAuthenticator 6.4

Fortinet NSE6_FAC-6.4

Version Demo

Total Demo Questions: 5

Total Premium Questions: 51

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

Topic Break Down

Topic	No. of Questions
Topic 1, Authentication	29
Topic 2, PKI	11
Topic 3, FSSO	3
Topic 4, Administration	8
Total	51

QUESTION NO: 1

Which two types of digital certificates can you create in Fortiauthenticator? (Choose two)

A. User certificate

B. Organization validation certificate

C. Third-party root certificate

D. Local service certificate

ANSWER: A D

Explanation:

FortiAuthenticator can create both a user certificate and a local service certificate. A user certificate is an identity certificate issued by the FortiAuthenticator certificate authority to a particular user, and it can support certificate-based authentication. This allows a user identity to be validated with a public-key certificate rather than relying solely on a password. User certificates are therefore appropriate for environments that use client-certificate authentication, including remote-access, wireless, or similar identity-based access workflows.

A local service certificate is created for FortiAuthenticator itself and is used to identify and secure services hosted by the appliance. It contains the appliance or service identity and associated private key material, enabling FortiAuthenticator to present a trusted certificate when clients connect to its services. Administrators can use this certificate for services such as the administrative HTTPS interface and other locally provided secure services, depending on the deployment configuration. Fortinet distinguishes these certificate purposes in its certificate-management documentation: user certificates represent issued user identities, while local service certificates secure the FortiAuthenticator service identity. See the FortiAuthenticator 6.4 Certificate Management documentation.

QUESTION NO: 2

An administrator is integrating FortiAuthenticator with an existing RADIUS server with the intent of eventually replacing the RADIUS server with FortiAuthenticator.

How can FortiAuthenticator help facilitate this process?

A. By configuring the RADIUS accounting proxy

B. By enabling automatic REST API calls from the RADIUS server

C. By enabling learning mode in the RADIUS server configuration

D. By importing the RADIUS user records

ANSWER: C

Explanation:

By enabling learning mode in the RADIUS server configuration is correct because it supports a staged migration from an existing RADIUS deployment to FortiAuthenticator. In this arrangement, FortiAuthenticator can act as the RADIUS server presented to authenticating devices while forwarding authentication requests to the existing, authoritative RADIUS server. When the remote server successfully authenticates a user, FortiAuthenticator learns the user credentials and creates a local user record. Subsequent authentication attempts can then be handled from FortiAuthenticator's local user database, reducing reliance on the legacy server over time.

This approach lets an administrator introduce FortiAuthenticator without requiring every user to be migrated manually before cutover. It also provides a practical transition path: existing credentials continue to work during the learning period, while FortiAuthenticator progressively builds the local credential store needed to assume the authentication role. After users have authenticated and been learned as needed, the organization can retire the prior RADIUS service with substantially less disruption. Learning mode is specifically documented as a RADIUS-service feature for obtaining and retaining user credentials from a remote RADIUS server during this type of migration. See the FortiAuthenticator 6.4 Administration Guide: Learning mode and the RADIUS service configuration documentation.

QUESTION NO: 3

An organization is deploying wireless 802.1X authentication. The security policy prohibits password-based authentication and requires both the wireless client and FortiAuthenticator to prove their identities with certificates.

Which EAP method should the administrator configure?

A. EAP-GTC

B. EAP-TLS

C. PEAP with MSCHAPv2

D. EAP-TTLS with PAP

ANSWER: B

Explanation:

EAP-TLS is correct because it performs mutual certificate-based authentication between the supplicant and the EAP server. The client presents its certificate to FortiAuthenticator, and FortiAuthenticator presents its EAP server certificate to the client. This meets the requirement to avoid password-based authentication.

PEAP and EAP-TTLS establish a TLS tunnel using a server certificate, but normally authenticate the user through an inner credential-based method. EAP-GTC is also a credential-based method and does not provide certificate-based mutual authentication.

QUESTION NO: 4

An administrator configures PEAP for a wireless network using FortiAuthenticator as the RADIUS server.

Which two statements about the PEAP deployment are true? (Choose two)

A. FortiAuthenticator must present an EAP server certificate

B. The client must always present a user certificate

C. An inner authentication method is used inside the TLS tunnel

D. The user password is sent without encryption to the RADIUS server

ANSWER: A C

Explanation:

PEAP requires FortiAuthenticator to present an EAP server certificate so that the supplicant can validate the identity of the authentication server before creating the protected tunnel. After the outer TLS tunnel is established, an inner authentication method, such as MSCHAPv2 or EAP-GTC, authenticates the user within that tunnel.

PEAP does not inherently require a client certificate; that requirement is characteristic of EAP-TLS. The user credentials are protected by the PEAP tunnel rather than being sent as clear-text credentials over the wireless network.

QUESTION NO: 5

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. Create an admin realm in the authentication policy

B. Specify the appropriate RADIUS clients in the authentication policy

C. Enable Adaptive Authentication in the portal policy

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

ANSWER: C

Explanation:

Enable Adaptive Authentication in the portal policy. Adaptive Authentication lets FortiAuthenticator apply authentication requirements according to the context of the access request, including whether the source network is trusted. An administrator can define trusted network locations and associate the appropriate adaptive-authentication behavior with the portal policy. When a user connects from a recognized secured network, FortiAuthenticator can accept the primary authentication factor without requiring the usual second factor. This permits a practical balance between security and usability: users remain subject to strong authentication when they connect from untrusted or unfamiliar locations, while access from an approved internal network can be streamlined. The trusted-network determination can use source IP information and, where configured, IP-based geolocation data. Adaptive Authentication therefore directly addresses the requirement to conditionally bypass two-factor authentication based on the network from which the user accesses the protected service. Fortinet documents Adaptive Authentication as part of its authentication-policy capabilities and describes its use for varying authentication requirements according to access context. See the FortiAuthenticator 6.4 Administration Guide: Adaptive Authentication and the FortiAuthenticator 6.4 Administration Guide.