Practice Exam Questions

NSE6_FAC-6.4

Fortinet NSE 6

FortiAuthenticator 6.4

EXAMKILLER

Help Pass Your Exam At First Try

Fortinet

Exam NSE6_FAC-6.4

Fortinet NSE 6 - FortiAuthenticator 6.4

Version: 3.0

[Total Questions: 47]

Question No : 1

Which two SAML roles can Fortiauthenticator be configured as? (Choose two)

A. Idendity provider
B. Principal
C. Assertion server
D. Service provider

Answer: A,D

Explanation: FortiAuthenticator can be configured as a SAML identity provider (IdP) or a SAML service provider (SP). As an IdP, FortiAuthenticator authenticates users and issues SAML assertions to SPs. As an SP, FortiAuthenticator receives SAML assertions from IdPs and grants access to users based on the attributes in the assertions. Principal and assertion server are not valid SAML roles. References: https://docs.fortinet.com/document/fortiauthenticator/6.4/administration-guide/372407/saml

Question No : 2

An administrator has an active directory (AD) server integrated with FortiAuthenticator. They want members of only specific AD groups to participate in FSSO with their corporate FortiGate firewalls.

How does the administrator accomplish this goal?

A. Configure a FortiGate filter on FortiAuthenticatoc
B. Configure a domain groupings list to identify the desired AD groups.
C. Configure fine-grained controls on FortiAuthenticator to designate AD groups.
D. Configure SSO groups and assign them to FortiGate groups.

Answer: D

Explanation:
To allow members of only specific AD groups to participate in FSSO with their corporate FortiGate firewalls, the administrator can configure SSO groups and assign them to FortiGate groups. SSO groups are groups of users or devices that are defined on FortiAuthenticator based on various criteria, such as user group membership, source IP address, MAC address, or device type. FortiGate groups are groups of users or devices that are defined on FortiGate based on various criteria, such as user group membership, firewall policy, or authentication method. By mapping SSO groups to FortiGate groups, the

administrator can control which users or devices can access the network resources protected by FortiGate.
References: https://docs.fortinet.com/document/fortiauthenticator/6.4.0/administration-guide/906179/single-sign-on#sso-groups

Question No : 3

What capability does the inbound proxy setting provide?

A. It allows FortiAuthenticator to determine the origin source IP address after traffic passes through a proxy for system access,
B. It allows FortiAuthenticator to act as a proxy for remote authentication servers.
C. It allows FortiAuthenticator the ability to round robin load balance remote authentication servers.
D. It allows FortiAuthenticator system access to authenticating users, based on a geo IP address designation.

Answer: A

Explanation:
The inbound proxy setting provides the ability for FortiAuthenticator to determine the origin source IP address after traffic passes through a proxy for system access. The inbound proxy setting allows FortiAuthenticator to use the X-Forwarded-For header in the HTTP request to identify the original client IP address. This can help FortiAuthenticator apply the correct authentication policy or portal policy based on the source IP address.
References: https://docs.fortinet.com/document/fortiauthenticator/6.4.0/administration-guide/906179/system-settings#inbound-proxy

Question No : 4

Which statement about the guest portal policies is true?

A. Guest portal policies apply only to authentication requests coming from unknown

RADIUS clients
B. Guest portal policies can be used only for BYODs
C. Conditions in the policy apply only to guest wireless users
D. All conditions in the policy must match before a user is presented with the guest portal

Answer: D

Explanation:

Guest portal policies are rules that determine when and how to present the guest portal to users who want to access the network. Each policy has a set of conditions that can be based on various factors, such as the source IP address, MAC address, RADIUS client, user agent, or SSID. All conditions in the policy must match before a user is presented with the guest portal. Guest portal policies can apply to any authentication request coming from any RADIUS client, not just unknown ones. They can also be used for any type of device, not just BYODs. They can also apply to wired or VPN users, not just wireless users.
References: https://docs.fortinet.com/document/fortiauthenticator/6.4/administration-guide/372404/guest-management/372406/portal-policies

Question No : 5

Which two statements about the EAP-TTLS authentication method are true? (Choose two)

A. Uses mutual authentication
B. Uses digital certificates only on the server side
C. Requires an EAP server certificate
D. Support a port access control (wired) solution only

Answer: B,C

Explanation:

EAP-TTLS is an authentication method that uses digital certificates only on the server side to establish a secure tunnel between the server and the client. The client does not need a certificate but can use any inner authentication method supported by the server, such as PAP, CHAP, MS-CHAP, or EAP-MD5. EAP-TTLS requires an EAP server certificate that is issued by a trusted CA and installed on the FortiAuthenticator device acting as the EAP server. EAP-TTLS supports both wireless and wired solutions for port access control.
References: https://docs.fortinet.com/document/fortiauthenticator/6.4/administration-guide/372412/eap-ttls

Question No : 6

Which network configuration is required when deploying FortiAuthenticator for portal services?

A. FortiAuthenticator must have the REST API access enable on port1
B. One of the DNS servers must be a FortiGuard DNS server
C. Fortigate must be setup as default gateway for FortiAuthenticator
D. Policies must have specific ports open between FortiAuthenticator and the authentication clients

Answer: D

Explanation: When deploying FortiAuthenticator for portal services, such as guest portal, sponsor portal, user portal or FortiToken activation portal, the network configuration must allow specific ports to be open between FortiAuthenticator and the authentication clients. These ports are:

- TCP 80 for HTTP access
- TCP 443 for HTTPS access
- TCP 389 for LDAP access
- TCP 636 for LDAPS access
- UDP 1812 for RADIUS authentication
- UDP 1813 for RADIUS accounting

References: https://docs.fortinet.com/document/fortiauthenticator/6.4.0/administration-guide/906179/portal-services#network-configuration

Question No : 7

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:

FortiAuthenticator can help facilitate the process of replacing an existing RADIUS server by enabling learning mode in the RADIUS server configuration. This allows FortiAuthenticator to learn user credentials from the existing RADIUS server and store them locally for future authentication requests2. This way, FortiAuthenticator can gradually take over the role of the RADIUS server without disrupting the user experience.

References: 2 https://docs.fortinet.com/document/fortiauthenticator/6.4.0/administration-guide/906179/radius-service#learning-mode

Question No : 8

A digital certificate, also known as an X.509 certificate, contains which two pieces of information? (Choose two.)

A. Issuer
B. Shared secret
C. Public key
D. Private key

Answer: A,C

Explanation:

A digital certificate, also known as an X.509 certificate, contains two pieces of information:

- Issuer, which is the identity of the certificate authority (CA) that issued the certificate
- Public key, which is the public part of the asymmetric key pair that is associated with the certificate subject

References: https://docs.fortinet.com/document/fortiauthenticator/6.4.0/administration-guide/906179/certificate-management#certificate-components

Question No : 9

Which two statements about the self-service portal are true? (Choose two)

A. Self-registration information can be sent to the user through email or SMS
B. Realms can be used to configure which seld-registered users or groups can authenticate on the network
C. Administrator approval is required for all self-registration
D. Authenticating users must specify domain name along with username

Answer: A,B

Explanation:

Two statements about the self-service portal are true:

- Self-registration information can be sent to the user through email or SMS using the notification templates feature. This feature allows administrators to customize the messages that are sent to users when they register or perform other actions on the self-service portal.
- Realms can be used to configure which self-registered users or groups can authenticate on the network using the realm-based authentication feature. This feature allows administrators to apply different authentication policies and settings to different groups of users based on their realm membership.

References: https://docs.fortinet.com/document/fortiauthenticator/6.4.0/administration-guide/906179/user-management#self-registration
https://docs.fortinet.com/document/fortiauthenticator/6.4.0/administration-guide/906179/user-management#realms

Question No : 10

An administrator wants to keep local CA cryptographic keys stored in a central location.

Which FortiAuthenticator feature would provide this functionality?

A. SCEP support
B. REST API
C. Network HSM
D. SFTP server

Answer: C

Explanation:
Network HSM is a feature that allows FortiAuthenticator to keep local CA cryptographic keys stored in a central location. HSM stands for Hardware Security Module, which is a physical device that provides secure storage and generation of cryptographic keys. Network HSM allows FortiAuthenticator to use an external HSM device to store and manage the private keys of its local CAs, instead of storing them locally on the FortiAuthenticator device.
References: https://docs.fortinet.com/document/fortiauthenticator/6.4.0/administration-guide/906179/certificate-management#network-hsm

Question No : 11

What are three key features of FortiAuthenticator? (Choose three)

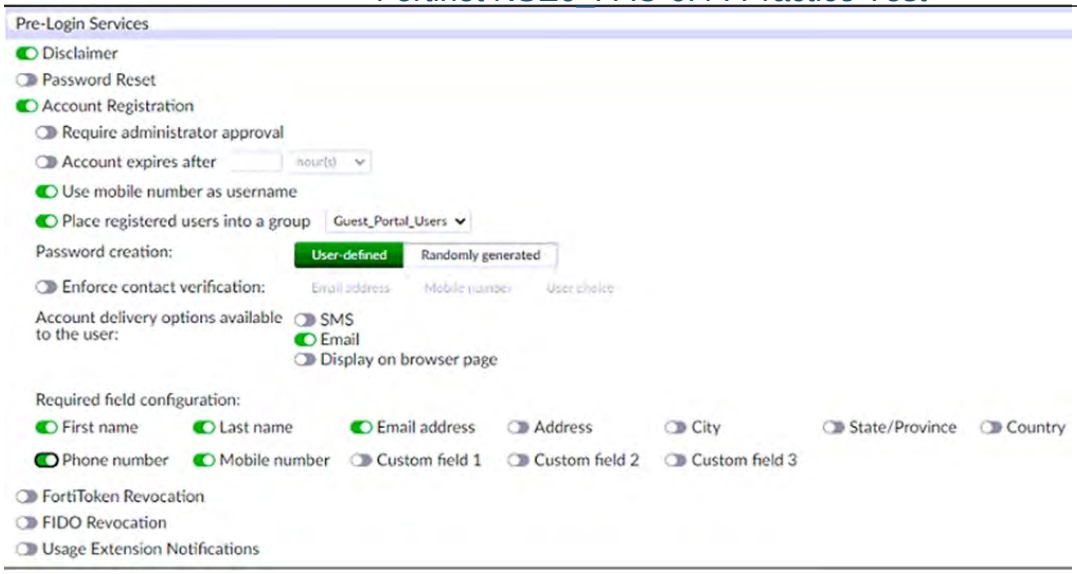
A. Identity management device
B. Log server
C. Certificate authority
D. Portal services
E. RSSO Server

Answer: A,C,D

Explanation: FortiAuthenticator is a user and identity management solution that provides strong authentication, wireless 802.1X authentication, certificate management, RADIUS AAA (authentication, authorization, and accounting), and Fortinet Single Sign-On (FSSO). It also offers portal services for guest management, self-service password reset, and device registration. It is not a log server or an RSSO server. References: https://docs.fortinet.com/document/fortiauthenticator/6.4/release-notes

Question No : 12

Examine the screenshot shown in the exhibit.



Which two statements regarding the configuration are true? (Choose two.)

A. All guest accounts created using the account registration feature will be placed under the Guest_Portal_Users group
B. All accounts registered through the guest portal must be validated through email
C. Guest users must fill in all the fields on the registration form
D. Guest user account will expire after eight hours

Answer: A,B

Explanation:

The screenshot shows that the account registration feature is enabled for the guest portal and that the guest group is set to Guest_Portal_Users. This means that all guest accounts created using this feature will be placed under that group1. The screenshot also shows that email validation is enabled for the guest portal and that the email validation link expires after 24 hours. This means that all accounts registered through the guest portal must be validated through email within that time frame1.
References: 1 https://docs.fortinet.com/document/fortiauthenticator/6.4.0/administration-guide/906179/guest-management#account-registration

Question No : 13

How can a SAML metada file be used?