Fortinet

Exam Questions NSE6_FAC-6.4

Fortinet NSE 6 - FortiAuthenticator 6.4

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1
At a minimum, which two configurations are required to enable guest portal services on FortiAuthenticator? (Choose two)

A. Configuring a portal policy
B. Configuring at least on post-login service
C. Configuring a RADIUS client
D. Configuring an external authentication portal

Answer: AB

Explanation:
enable guest portal services on FortiAuthenticator, you need to configure a portal policy that defines the conditions for presenting the guest portal to users and the authentication methods to use. You also need to configure at least one post-login service that defines what actions to take after a user logs in successfully, such as sending an email confirmation, assigning a VLAN, or creating a user account. Configuring a RADIUS client or an external authentication portal are optional steps that depend on your network setup and requirements. References:
https://docs.fortinet.com/document/fortiauthenticator/6.4/administration-guide/372404/guest-management

NEW QUESTION 2
Which two protocols are the default management access protocols for administrative access for FortiAuthenticator? (Choose two)

A. Telnet
B. HTTPS
C. SSH
D. SNMP

Answer: BC

Explanation:
HTTPS and SSH are the default management access protocols for administrative access for FortiAuthenticator. HTTPS allows administrators to access the web-based GUI of FortiAuthenticator using a web browser and a secure connection. SSH allows administrators to access the CLI of FortiAuthenticator using an SSH client and an encrypted connection. Both protocols require the administrator to enter a valid username and password to log in.
References:
https://docs.fortinet.com/document/fortiauthenticator/6.4.0/administration-guide/906179/system-settings#manag

NEW QUESTION 3
Which three of the following can be used as SSO sources? (Choose three)

A. FortiClient SSO Mobility Agent
B. SSH Sessions
C. FortiAuthenticator in SAML SP role
D. Fortigate
E. RADIUS accounting

Answer: ADE

Explanation:
FortiAuthenticator supports various SSO sources that can provide user identity information to other devices in the network, such as FortiGate firewalls or FortiAnalyzer log servers. Some of the supported SSO sources are:

- FortiClient SSO Mobility Agent: A software agent that runs on Windows devices and sends user login information to FortiAuthenticator.
- FortiGate: A firewall device that can send user login information from various sources, such as FSSO agents, captive portals, VPNs, or LDAP servers, to FortiAuthenticator.
- RADIUS accounting: A protocol that can send user login information from RADIUS servers or clients, such as wireless access points or VPN concentrators, to FortiAuthenticator.

SSH sessions and FortiAuthenticator in SAML SP role are not valid SSO sources because they do not provide user identity information to other devices in the network. References: https://docs.fortinet.com/document/fortiauthenticator/6.4/administration-guide/372410/single-sign-on

NEW QUESTION 4
You are an administrator for a large enterprise and you want to delegate the creation and management of guest users to a group of sponsors.
How would you associate the guest accounts with individual sponsors?

A. As an administrator, you can assign guest groups to individual sponsors.
B. Guest accounts are associated with the sponsor that creates the guest account.
C. You can automatically add guest accounts to groups associated with specific sponsors.
D. Select the sponsor on the guest portal, during registration.

Answer: B

Explanation:
Guest accounts are associated with the sponsor that creates the guest account. A sponsor is a user who has permission to create and manage guest accounts on behalf of other users3. A sponsor can create guest accounts using the sponsor portal or the REST API3. The sponsor's username is recorded as a field in the guest account's profile3.
References: 3 https://docs.fortinet.com/document/fortiauthenticator/6.4.0/administration-guide/906179/guest

NEW QUESTION 5
Which two capabilities does FortiAuthenticator offer when acting as a self-signed or local CA? (Choose two)

A. Validating other CA CRLs using OSCP
B. Importing other CA certificates and CRLs
C. Merging local and remote CRLs using SCEP
D. Creating, signing, and revoking of X.509 certificates

Answer: BD

Explanation:
FortiAuthenticator can act as a self-signed or local CA that can issue certificates to users, devices, or other CAs. It can also import other CA certificates and CRLs to trust them and validate their certificates. It can also create, sign, and revoke X.509 certificates for various purposes, such as VPN authentication, web server encryption, or wireless security. It cannot validate other CA CRLs using OCSP or merge local and remote CRLs using SCEP because these are protocols that require communication with external CAs. References: https://docs.fortinet.com/document/fortiauthenticator/6.4/administration-guide/372408/certificate-management

NEW QUESTION 6
At a minimum, which two configurations are required to enable guest portal services on FortiAuthenticator? (Choose two)

A. Configuring a portal policy
B. Configuring at least on post-login service
C. Configuring a RADIUS client
D. Configuring an external authentication portal

Answer: AB

Explanation:
To enable guest portal services on FortiAuthenticator, you need to configure a portal policy that defines the conditions for presenting the guest portal to users and the authentication methods to use. You also need to configure at least one post-login service that defines what actions to take after a user logs in successfully, such as sending an email confirmation, assigning a VLAN, or creating a user account. Configuring a RADIUS client or an external authentication portal are optional steps that depend on your network setup and requirements. References:
https://docs.fortinet.com/document/fortiauthenticator/6.4/administration-guide/372404/guest-management

NEW QUESTION 7
You are the administrator of a large network that includes a large local user datadabase on the current Fortiauthenticatior. You want to import all the local users into a new Fortiauthenticator device.
Which method should you use to migrate the local users?

A. Import users using RADIUS accounting updates.
B. Import the current directory structure.
C. Import users from RADUIS.
D. Import users using a CSV file.

Answer: D

Explanation:
The best method to migrate local users from one FortiAuthenticator device to another is to export the users from the current device as a CSV file and then import the CSV file into the new device. This method preserves all the user attributes and settings and allows you to modify them if needed before importing. The other methods are not suitable for migrating local users because they either require an external RADIUS server or do not transfer all the user information. References:
https://docs.fortinet.com/document/fortiauthenticator/6.4/administration-guide/372409/user-management

NEW QUESTION 8
Which of the following is an OATH-based standard to generate event-based, one-time password tokens?

A. HOTP
B. SOTP
C. TOTP
D. OLTP

Answer: A

NEW QUESTION 9
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: BC

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

NEW QUESTION 10
Which two features of FortiAuthenticator are used for EAP deployment? (Choose two)

A. Certificate authority
B. LDAP server
C. MAC authentication bypass
D. RADIUS server

Answer: AD

Explanation:
Two features of FortiAuthenticator that are used for EAP deployment are certificate authority and RADIUS server. Certificate authority allows FortiAuthenticator to issue and manage digital certificates for EAP methods that require certificate-based authentication, such as EAP-TLS or PEAP-EAP-TLS. RADIUS server allows FortiAuthenticator to act as an authentication server for EAP methods that use RADIUS as a transport protocol, such as EAP-GTC or PEAP-MSCHAPV2.
References:
https://docs.fortinet.com/document/fortiauthenticator/6.4.0/administration-guide/906179/wireless-802-1x-authen

NEW QUESTION 10
Which EAP method is known as the outer authentication method?

A. PEAP
B. EAP-GTC
C. EAP-TLS
D. MSCHAPV2

Answer: A

Explanation:
PEAP is known as the outer authentication method because it establishes a secure tunnel between the client and the server using TLS. The inner authentication method, such as EAP-GTC, EAP-TLS, or MSCHAPV2, is then used to authenticate the client within the tunnel.
References:
https://docs.fortinet.com/document/fortiauthenticator/6.4.0/administration-guide/906179/wireless-802-1x-authen

NEW QUESTION 11
Which statement about the assignment of permissions for sponsor and administrator accounts is true?

A. Only administrator accounts permissions are assigned using admin profiles.
B. Sponsor permissions are assigned using group settings.
C. Administrator capabilities are assigned by applying permission sets to admin groups.
D. Both sponsor and administrator account permissions are assigned using admin profiles.

Answer: D

Explanation:
Both sponsor and administrator account permissions are assigned using admin profiles. An admin profile is a set of permissions that defines what actions an administrator or a sponsor can perform on FortiAuthenticator. An admin profile can be assigned to an admin group or an individual admin user. A sponsor is a special type of admin user who can create and manage guest accounts on behalf of other users.
References:
https://docs.fortinet.com/document/fortiauthenticator/6.4.0/administration-guide/906179/administrators#admin-p

NEW QUESTION 15
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: AB

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-
https://docs.fortinet.com/document/fortiauthenticator/6.4.0/administration-guide/906179/user-management#real

NEW QUESTION 20
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

NEW QUESTION 23
Which option correctly describes an SP-initiated SSO SAML packet flow for a host without a SAML assertion?

A. Service provider contacts idendity provider, idendity provider validates principal for service provider, service provider establishes communication with principal
B. Principal contacts idendity provider and is redirected to service provider, principal establishes connection with service provider, service provider validates authentication with identify provider
C. Principal contacts service provider, service provider redirects principal to idendity provider, after succesfull authentication identify provider redirects principal to service provider
D. Principal contacts idendity provider and authenticates, identity provider relays principal to service provider after valid authentication

Answer: C

Explanation:
SP-initiated SSO SAML packet flow for a host without a SAML assertion is as follows:
- Principal contacts service provider, requesting access to a protected resource.
- Service provider redirects principal to identity provider, sending a SAML authentication request.
- Principal authenticates with identity provider using their credentials.
- After successful authentication, identity provider redirects principal back to service provider, sending a SAML response with a SAML assertion containing the principal's attributes.
- Service provider validates the SAML response and assertion, and grants access to the principal.

References:
https://docs.fortinet.com/document/fortiauthenticator/6.4.0/administration-guide/906179/saml-service-provider#

NEW QUESTION 26
Which behaviors exist for certificate revocation lists (CRLs) on FortiAuthenticator? (Choose two)

A. CRLs contain the serial number of the certificate that has been revoked
B. Revoked certificates are automaticlly placed on the CRL
C. CRLs can be exported only through the SCEP server
D. All local CAs share the same CRLs

Answer: AB

Explanation:
CRLs are lists of certificates that have been revoked by the issuing CA and should not be trusted by any entity. CRLs contain the serial number of the certificate that has been revoked, the date and time of revocation, and the reason for revocation. Revoked certificates are automatically placed on the CRL by the CA and the CRL is updated periodically. CRLs can be exported through various methods, such as HTTP, LDAP, or SCEP. Each local CA has its own CRL that is specific to its issued certificates. References:
https://docs.fortinet.com/document/fortiauthenticator/6.4/administration-guide/372408/certificate-management/3

NEW QUESTION 28
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: AD

Explanation:
FortiAuthenticator can create two types of digital certificates: user certificates and local service certificates. User certificates are issued to users or devices for authentication purposes, such as VPN, wireless, or web access. Local service certificates are issued to FortiAuthenticator itself for securing its own services, such as HTTPS, RADIUS, or LDAP.
References:
https://docs.fortinet.com/document/fortiauthenticator/6.4.0/administration-guide/906179/certificate-management

NEW QUESTION 33
.....

Relate Links

100% Pass Your NSE6_FAC-6.4 Exam with Exambible Prep Materials

https://www.exambible.com/NSE6_FAC-6.4-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/