Up-to-date Questions and Answers from authentic resources to improve knowledge and pass the exam at very first attempt. ----- Guaranteed.

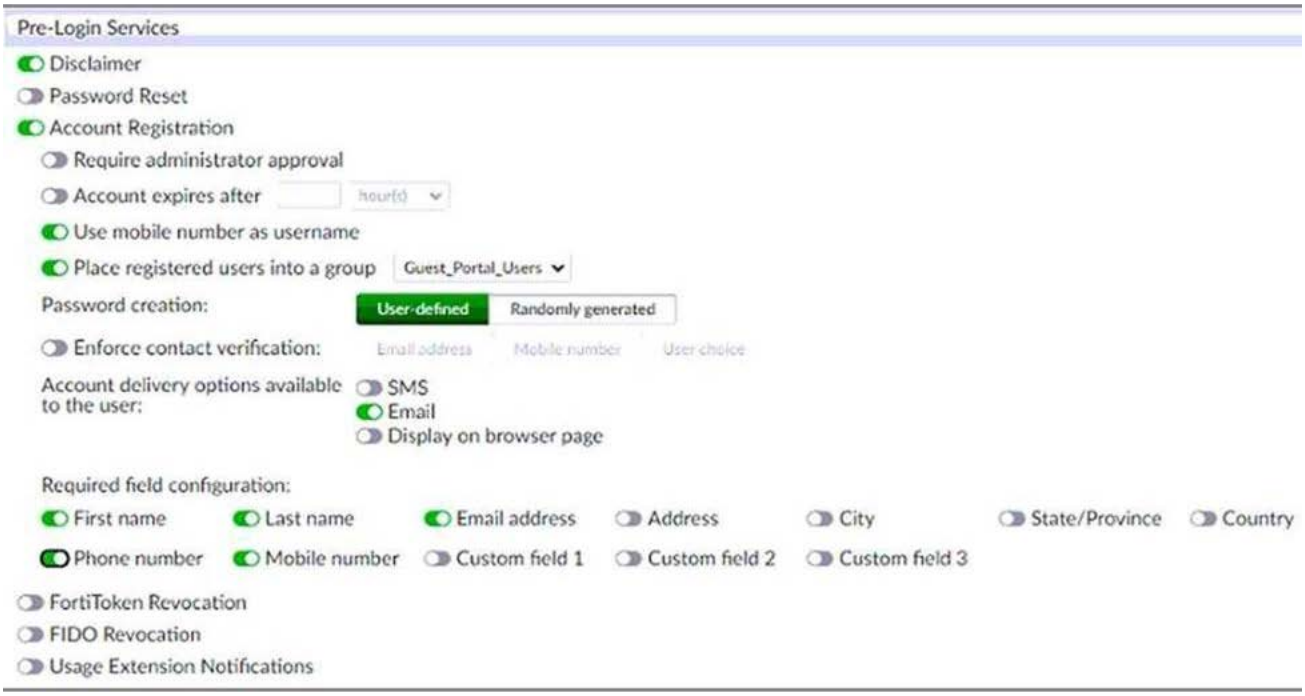
Fortinet

NSE6_FAC-6.4

NSE 6 - FortiAuthenticator 6.4

Question: 1

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.

Reference: 1 https://docs.fortinet.com/document/fortiauthenticator/6.4.0/administration-guide/906179/guest-management#account-registration

Question: 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:

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.

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

Question: 3

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 sponsorâs username is recorded as a field in the guest accountâs profile3.

Reference: 3 https://docs.fortinet.com/document/fortiauthenticator/6.4.0/administration-guide/906179/guest-management#sponsors

Question: 4

You are a Wi-Fi provider and host multiple domains.

How do you delegate user accounts, user groups and permissions per domain when they are authenticating on a single FortiAuthenticator device?

A. Create realms.
B. Create user groups

C. Create multiple directory trees on FortiAuthenticator
D. Automatically import hosts from each domain as they authenticate.

Answer: A

Explanation:

Realms are a way to delegate user accounts, user groups and permissions per domain when they are authenticating on a single FortiAuthenticator device. A realm is a logical grouping of users and groups based on a common attribute, such as a domain name or an IP address range. Realms allow administrators to apply different authentication policies and settings to different groups of users based on their realm membership.

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

Question: 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:

Adaptive Authentication is a feature that allows administrators to bypass the need for two-factor authentication for users accessing from specific secured networks. Adaptive Authentication uses geolocation information from IP addresses to determine whether a user is accessing from a trusted network or not. If the user is accessing from a trusted network, FortiAuthenticator can skip the second factor of authentication and grant access based on the first factor only.

Reference: https://docs.fortinet.com/document/fortiauthenticator/6.4.0/administration-guide/906179/authentication-policies#adaptive-authentication

Question: 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

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

Question: 7

You are a FortiAuthenticator administrator for a large organization. Users who are configured to use FortiToken 200 for two-factor authentication can no longer authenticate. You have verified that only the users with two-factor authentication are experiencing the issue.

What can cause this issue?

A. FortiToken 200 license has expired
B. One of the FortiAuthenticator devices in the active-active cluster has failed
C. Time drift between FortiAuthenticator and hardware tokens
D. FortiAuthenticator has lost contact with the FortiToken Cloud servers

Answer: C

Explanation:

One possible cause of the issue is time drift between FortiAuthenticator and hardware tokens. Time drift occurs when the internal clocks of FortiAuthenticator and hardware tokens are not synchronized. This can result in mismatched one-time passwords (OTPs) generated by the hardware tokens and expected by FortiAuthenticator. To prevent this issue, FortiAuthenticator provides a time drift tolerance option that allows a certain number of seconds of difference between the clocks.

Reference: https://docs.fortinet.com/document/fortiauthenticator/6.4.0/administration-guide/906179/two-factor-authentication#time-drift-tolerance

Question: 8

Why would you configure an OCSP responder URL in an end-entity certificate?

A. To designate the SCEP server to use for CRL updates for that certificate
B. To identify the end point that a certificate has been assigned to
C. To designate a server for certificate status checking
D. To provide the CRL location for the certificate

Answer: C

Explanation:

An OCSP responder URL in an end-entity certificate is used to designate a server for certificate status checking. OCSP stands for Online Certificate Status Protocol, which is a method of verifying whether a certificate is valid or revoked in real time. An OCSP responder is a server that responds to OCSP requests from clients with the status of the certificate in question. The OCSP responder URL in an end-entity certificate points to the location of the OCSP responder that can provide the status of that certificate.

Reference: https://docs.fortinet.com/document/fortiauthenticator/6.4.0/administration-guide/906179/certificate-management#ocsp-responder

Question: 9

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.

Reference: https://docs.fortinet.com/document/fortiauthenticator/6.4.0/administration-guide/906179/certificate-management#network-hsm

Question: 10

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 principalâs attributes.

Service provider validates the SAML response and assertion, and grants access to the principal.

Reference: https://docs.fortinet.com/document/fortiauthenticator/6.4.0/administration-guide/906179/saml-service-provider#sp-initiated-sso

Question: 11

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 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.

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

Question: 12

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.

Reference: https://docs.fortinet.com/document/fortiauthenticator/6.4.0/administration-guide/906179/wireless-802-1x-authentication#peap

Question: 13

You want to monitor FortiAuthenticator system information and receive FortiAuthenticator traps through SNMP.

Which two configurations must be performed after enabling SNMP access on the FortiAuthenticator interface? (Choose two)

A. Enable logging services
B. Set the tresholds to trigger SNMP traps
C. Upload management information base (MIB) files to SNMP server
D. Associate an ASN, 1 mapping rule to the receiving host

Answer: A,B,C

Explanation:

To monitor FortiAuthenticator system information and receive FortiAuthenticator traps through SNMP, two configurations must be performed after enabling SNMP access on the FortiAuthenticator interface:

Set the thresholds to trigger SNMP traps for various system events, such as CPU usage, disk usage, memory usage, or temperature.

Upload management information base (MIB) files to SNMP server to enable the server to interpret the SNMP traps sent by FortiAuthenticator.

Reference: https://docs.fortinet.com/document/fortiauthenticator/6.4.0/administration-guide/906179/system-settings#snmp

Question: 14

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: A,D

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.

Reference: https://docs.fortinet.com/document/fortiauthenticator/6.4.0/administration-guide/906179/wireless-802-1x-authentication

Question: 15

How can a SAML metada file be used?

A. To defined a list of trusted user names
B. To import the required IDP configuration
C. To correlate the IDP address to its hostname
D. To resolve the IDP realm for authentication

Answer: B

Explanation:

A SAML metadata file can be used to import the required IDP configuration for SAML service provider mode. A SAML metadata file is an XML file that contains information about the identity provider (IDP) and the service provider (SP), such as their entity IDs, endpoints, certificates, and attributes. By importing a SAML metadata file from the IDP, FortiAuthenticator can automatically configure the necessary settings for SAML service provider mode.

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

SAMPLE QUESTIONS

These questions are for demo purpose only. ***Full version*** *is up to date and contains actual questions and answers.*

Killexams.com is an online platform that offers a wide range of services related to certification exam preparation. The platform provides actual questions, exam dumps, and practice tests to help individuals prepare for various certification exams with confidence. Here are some key features and services offered by Killexams.com:

Actual Exam Questions*: Killexams.com provides actual exam questions that are experienced in test centers. These questions are updated regularly to ensure they are up-to-date and relevant to the latest exam syllabus. By studying these actual questions, candidates can familiarize themselves with the content and format of the real exam.*

Exam Dumps*: Killexams.com offers exam dumps in PDF format. These dumps contain a comprehensive collection of questions and answers that cover the exam topics. By using these dumps, candidates can enhance their knowledge and improve their chances of success in the certification exam.*

Practice Tests*: Killexams.com provides practice tests through their desktop VCE exam simulator and online test engine. These practice tests simulate the real exam environment and help candidates assess their readiness for the actual exam. The practice tests cover a wide range of questions and enable candidates to identify their strengths and weaknesses.*

Guaranteed Success*: Killexams.com offers a success guarantee with their exam dumps. They claim that by using their materials, candidates will pass their exams on the first attempt or they will refund the purchase price. This guarantee provides assurance and confidence to individuals preparing for certification exams.*

Updated Content: *Killexams.com regularly updates its question bank and exam dumps to ensure that they are current and reflect the latest changes in the exam syllabus. This helps candidates stay up-to-date with the exam content and increases their chances of success.*

Technical Support*: Killexams.com provides free 24x7 technical support to assist candidates with any queries or issues they may encounter while using their services. Their certified experts are available to provide guidance and help candidates throughout their exam preparation journey.*