Exam Questions NSE6_FAC-6.4

Fortinet NSE 6 - FortiAuthenticator 6.4

https://www.2passeasy.com/dumps/NSE6_FAC-6.4/

NEW QUESTION 1
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 2
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.
References:
https://docs.fortinet.com/document/fortiauthenticator/6.4.0/administration-guide/906179/certificate-management

NEW QUESTION 3
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.
References:
https://docs.fortinet.com/document/fortiauthenticator/6.4.0/administration-guide/906179/saml-service-provider#

NEW QUESTION 4
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#networ

NEW QUESTION 5

What happens when a certificate is revoked? (Choose two)

A. Revoked certificates cannot be reinstated for any reason
B. All certificates signed by a revoked CA certificate are automatically revoked
C. Revoked certificates are automatically added to the CRL
D. External CAs will priodically query Fortiauthenticator and automatically download revoked certificates

Answer: BC

Explanation:
When a certificate is revoked, it means that it is no longer valid and should not be trusted by any entity. Revoked certificates are automatically added to the certificate revocation list (CRL) which is published by the issuing CA and can be checked by other parties. If a CA certificate is revoked, all certificates signed by that CA are also revoked and added to the CRL. Revoked certificates can be reinstated if the reason for revocation is resolved, such as a compromised private key being recovered or a misissued certificate being corrected. External CAs do not query FortiAuthenticator for revoked certificates, but they can use protocols such as SCEP or OCSP to exchange certificate information with FortiAuthenticator. References: https://docs.fortinet.com/document/fortiauthenticator/6.4/administration-guide/372408/certificate-management

NEW QUESTION 6
Which two are supported captive or guest portal authentication methods? (Choose two)

A. LinkedIn
B. Apple ID
C. Instagram
D. Email

Answer: AD

Explanation:
FortiAuthenticator supports various captive or guest portal authentication methods, including social media login with LinkedIn, Facebook, Twitter, Google+, or WeChat; email verification; SMS verification; voucher code; username and password; and MAC address bypass. Apple ID and Instagram are not supported as authentication methods. References:
https://docs.fortinet.com/document/fortiauthenticator/6.4/administration-guide/372404/guest-management/37240

NEW QUESTION 7
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.
References:
https://docs.fortinet.com/document/fortiauthenticator/6.4.0/administration-guide/906179/authentication-policies

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
When configuring syslog SSO, which three actions must you take, in addition to enabling the syslog SSO method? (Choose three.)

A. Enable syslog on the FortiAuthenticator interface.
B. Define a syslog source.
C. Select a syslog rule for message parsing.
D. Set the same password on both the FortiAuthenticator and the syslog server.
E. Set the syslog UDP port on FortiAuthenticator.

Answer: BCE

Explanation:
To configure syslog SSO, three actions must be taken, in addition to enabling the syslog SSO method:
- Define a syslog source, which is a device that sends syslog messages to FortiAuthenticator containing user logon or logoff information.
- Select a syslog rule for message parsing, which is a predefined or custom rule that defines how to extract the user name, IP address, and logon or logoff action from the syslog message.

- Set the syslog UDP port on FortiAuthenticator, which is the port number that FortiAuthenticator listens on for incoming syslog messages.

References:
https://docs.fortinet.com/document/fortiauthenticator/6.4.0/administration-guide/906179/single-sign-on#syslog-s

NEW QUESTION 10
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: AB

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

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 method is the most secure way of delivering FortiToken data once the token has been seeded?

A. Online activation of the tokens through the FortiGuard network
B. Shipment of the seed files on a CD using a tamper-evident envelope
C. Using the in-house token provisioning tool
D. Automatic token generation using FortiAuthenticator

Answer: A

Explanation:
Online activation of the tokens through the FortiGuard network is the most secure way of delivering FortiToken data once the token has been seeded because it eliminates the risk of seed files being compromised during transit or storage. The other methods involve physical or manual delivery of seed files which can be intercepted, lost, or stolen. References: https://docs.fortinet.com/document/fortiauthenticator/6.4/administration-guide/372403/fortitoken

NEW QUESTION 15
You are the administrator of a global enterprise with three FortiAuthenticator devices. You would like to deploy them to provide active-passive HA at headquarters, with geographically distributed load balancing.
What would the role settings be?

A. One standalone and two load balancersB One standalone primary, one cluster member, and one load balancer
B. Two cluster members and one backup
C. Two cluster members and one load balancer

Answer: B

Explanation:
To deploy three FortiAuthenticator devices to provide active-passive HA at headquarters, with geographically distributed load balancing, the role settings would be:

- One standalone primary, which acts as the master device for HA and load balancing
- One cluster member, which acts as the backup device for HA and load balancing
- One load balancer, which acts as a remote device that forwards authentication requests to the primary or cluster member device

References:
https://docs.fortinet.com/document/fortiauthenticator/6.4.0/administration-guide/906179/high-availability#ha-an

NEW QUESTION 18
Which interface services must be enabled for the SCEP client to connect to Authenticator?

A. OCSP
B. REST API

C. SSH
D. HTTP/HTTPS

Answer: D

Explanation:
HTTP/HTTPS are the interface services that must be enabled for the SCEP client to connect to FortiAuthenticator. SCEP stands for Simple Certificate Enrollment Protocol, which is a method of requesting and issuing digital certificates over HTTP or HTTPS. FortiAuthenticator supports SCEP as a certificate authority (CA) and can process SCEP requests from SCEP clients. To enable SCEP on FortiAuthenticator, the HTTP or HTTPS service must be enabled on the interface that receives the SCEP requests.
References:
https://docs.fortinet.com/document/fortiauthenticator/6.4.0/administration-guide/906179/certificate-management

NEW QUESTION 21
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.
References:
https://docs.fortinet.com/document/fortiauthenticator/6.4.0/administration-guide/906179/two-factor-authenticati

NEW QUESTION 23
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 26
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 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 30
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual NSE6_FAC-6.4 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the NSE6_FAC-6.4 Product From:

https://www.2passeasy.com/dumps/NSE6_FAC-6.4/

Money Back Guarantee

NSE6_FAC-6.4 Practice Exam Features:

* NSE6_FAC-6.4 Questions and Answers Updated Frequently

* NSE6_FAC-6.4 Practice Questions Verified by Expert Senior Certified Staff

* NSE6_FAC-6.4 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* NSE6_FAC-6.4 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year