

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

Which FSSO discovery method transparently detects logged off users without having to rely on external features such as WMI polling?

- A. Windows AD polling
- B. FortiClient SSO Mobility Agent
- C. Radius Accounting
- D. DC Polling

Answer: B

Explanation:

FortiClient SSO Mobility Agent is a FSSO discovery method that transparently detects logged off users without having to rely on external features such as WMI polling. FortiClient SSO Mobility Agent is a software agent that runs on Windows devices and communicates with FortiAuthenticator to provide FSSO information. The agent can detect user logon and logoff events without using WMI polling, which can reduce network traffic and improve performance.

References:

<https://docs.fortinet.com/document/fortiauthenticator/6.4.0/administration-guide/906179/single-sign-on#forticlie>

NEW QUESTION 4

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 5

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/radiu>

NEW QUESTION 6

A system administrator wants to integrate FortiAuthenticator with an existing identity management system with the goal of authenticating and deauthenticating users into FSSO.

What feature does FortiAuthenticator offer for this type of integration?

- A. The ability to import and export users from CSV files
- B. RADIUS learning mode for migrating users
- C. REST API
- D. SNMP monitoring and traps

Answer: C

Explanation:

REST API is a feature that allows FortiAuthenticator to integrate with an existing identity management system with the goal of authenticating and deauthenticating users into FSSO. REST API stands for Representational State Transfer Application Programming Interface, which is a method of exchanging data between different systems using HTTP requests and responses. FortiAuthenticator provides a REST API that can be used by external systems to perform various actions, such as creating, updating, deleting, or querying users and groups, or sending FSSO logon or logoff events.

References: <https://docs.fortinet.com/document/fortiauthenticator/6.4.0/administration-guide/906179/rest-api>

NEW QUESTION 7

How can a SAML metadata 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 8

When you are setting up two FortiAuthenticator devices in active-passive HA, which HA role must you select on the master FortiAuthenticator?

- A. Active-passive master
- B. Standalone master
- C. Cluster member
- D. Load balancing master

Answer: A

Explanation:

When you are setting up two FortiAuthenticator devices in active-passive HA, you need to select the active-passive master role on the master FortiAuthenticator device. This role means that the device will handle all requests and synchronize data with the slave device until a failover occurs. The slave device must be configured as an active-passive slave role. The other roles are used for different HA modes, such as standalone (no HA), cluster (active-active), or load balancing (active-active with load balancing). References:

<https://docs.fortinet.com/document/fortiauthenticator/6.4/administration-guide/372411/high-availability>

NEW QUESTION 9

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 10

Which two statement about the RADIUS service on FortiAuthenticator are true? (Choose two)

- A. Two-factor authentication cannot be enforced when using RADIUS authentication
- B. RADIUS users can migrated to LDAP users
- C. Only local users can be authenticated through RADIUS
- D. FortiAuthenticator answers only to RADIUS client that are registered with FortiAuthenticator

Answer: BD

Explanation:

Two statements about the RADIUS service on FortiAuthenticator are true:

- RADIUS users can be migrated to LDAP users using the RADIUS learning mode feature. This feature allows FortiAuthenticator to learn user credentials from an existing RADIUS server and store them locally as LDAP users for future authentication requests.
- FortiAuthenticator answers only to RADIUS clients that are registered with FortiAuthenticator. A RADIUS client is a device that sends RADIUS authentication or accounting requests to FortiAuthenticator. A RADIUS client must be added and configured on FortiAuthenticator before it can communicate with it.

References:

<https://docs.fortinet.com/document/fortiauthenticator/6.4.0/administration-guide/906179/radius-service>

NEW QUESTION 10

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 11

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: AC

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>

NEW QUESTION 14

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 19

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 23

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 27

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: ACD

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>

NEW QUESTION 30

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 31

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 32

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

- A. Service provider contacts identity provider, identity provider validates principal for service provider, service provider establishes communication with principal
- B. Principal contacts identity provider and is redirected to service provider, principal establishes connection with service provider, service provider validates authentication with identity provider
- C. Principal contacts service provider, service provider redirects principal to identity provider, after successful authentication identity provider redirects principal to service provider
- D. Principal contacts identity 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 36

Which statement about captive portal policies is true, assuming a single policy has been defined?

- A. All conditions in the policy must match before a user is presented with the captive portal.
- B. Conditions in the policy apply only to wireless users.
- C. Portal policies can be used only for BYODs.

Answer: B

Explanation:

Captive portal policies are used to define the conditions and settings for presenting a captive portal to users who need to authenticate before accessing the network. A captive portal policy consists of a set of conditions and a set of actions. The conditions can be based on various attributes, such as source IP address, MAC address, user group, device type, or RADIUS client. The actions can include redirecting the user to a specific portal, applying a specific authentication method, or assigning a specific VLAN or firewall policy. A single policy can have multiple conditions, and all conditions in the policy must match before a user is presented with the captive portal.

References:

<https://docs.fortinet.com/document/fortiauthenticator/6.4.0/administration-guide/906179/portal-services#captive>

NEW QUESTION 41

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 automatically 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 43

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 47
.....

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