NSE6_FAC-6.4 Free Certification Exam Material from Exams4sures with 49 Questions [Q29-Q45

NSE6_FAC-6.4 Free Certification Exam Material from Exams4sures with 49 Questions
Use Real NSE6_FAC-6.4 - 100% Cover Real Exam Questions

The Fortinet NSE6_FAC-6.4 exam comprises of 35 multiple choice questions, which a candidate must complete in 60 minutes. The passing criteria for the exam is a minimum score of 60%. NSE6_FAC-6.4 exam is available in English and is conducted at Fortinet certified training centers worldwide.

Fortinet NSE6_FAC-6.4 certification exam is a comprehensive exam that covers a wide range of topics related to FortiAuthenticator 6.4. NSE6_FAC-6.4 exam consists of multiple-choice questions and is designed to test the candidate's ability to design, implement and manage FortiAuthenticator 6.4 in a network environment. NSE6_FAC-6.4 exam is proctored and is available in several languages.

NEW QUESTION 29

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

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.

NEW QUESTION 30

Which two SAML roles can Fortiauthenticator be configured as? (Choose two)
* Idendity provider
* Principal
* Assertion server
* Service provider

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. Reference: https://docs.fortinet.com/document/fortiauthenticator/6.4/administration-guide/372407/saml

NEW QUESTION 31

Which statement about the guest portal policies is true?
* Guest portal policies apply only to authentication requests coming from unknown RADIUS clients
* Guest portal policies can be used only for BYODs
* Conditions in the policy apply only to guest wireless users
* All conditions in the policy must match before a user is presented with the guest portal

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. Reference: https://docs.fortinet.com/document/fortiauthenticator/6.4/administration-guide/372404/guest-management/372406/portal-policies

NEW QUESTION 32

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?
* One standalone and two load balancers
* One standalone primary, one cluster member, and one load balancer
* Two cluster members and one backup
* Two cluster members and one load balancer

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

NEW QUESTION 33

At a minimum, which two configurations are required to enable guest portal services on FortiAuthenticator? (Choose two)
* Configuring a portal policy
* Configuring at least on post-login service
* Configuring a RADIUS client
* Configuring an external authentication portal

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. Reference: https://docs.fortinet.com/document/fortiauthenticator/6.4/administration-guide/372404/guest-management

NEW QUESTION 34

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

Which FortiAuthenticator feature would provide this functionality?
* SCEP support
* REST API
* Network HSM
* SFTP server

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.

NEW QUESTION 35

How can a SAML metada file be used?
* To defined a list of trusted user names
* To import the required IDP configuration
* To correlate the IDP address to its hostname
* To resolve the IDP realm for authentication

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.

NEW QUESTION 36

Which two statements about the self-service portal are true? (Choose two)
* Self-registration information can be sent to the user through email or SMS
* Realms can be used to configure which seld-registered users or groups can authenticate on the network
* Administrator approval is required for all self-registration

* Authenticating users must specify domain name along with username

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.

NEW QUESTION 37

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?

* Create realms.
* Create user groups
* Create multiple directory trees on FortiAuthenticator
* Automatically import hosts from each domain as they authenticate.

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.

NEW QUESTION 38

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

* OCSP
* REST API
* SSH
* HTTP/HTTPS

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.

NEW QUESTION 39

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

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

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.

NEW QUESTION 40

A digital certificate, also known as an X.509 certificate, contains which two pieces of information? (Choose two.)
* Issuer
* Shared secret
* Public key
* Private key
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

NEW QUESTION 41

What are three key features of FortiAuthenticator? (Choose three)
* Identity management device
* Log server
* Certificate authority
* Portal services
* RSSO Server
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. Reference: https://docs.fortinet.com/document/fortiauthenticator/6.4/release-notes

NEW QUESTION 42

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?
* The ability to import and export users from CSV files
* RADIUS learning mode for migrating users
* REST API
* SNMP monitoring and traps
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.

NEW QUESTION 43

Which method is the most secure way of delivering FortiToken data once the token has been seeded?
* Online activation of the tokens through the FortiGuard network
* Shipment of the seed files on a CD using a tamper-evident envelope
* Using the in-house token provisioning tool
* Automatic token generation using FortiAuthenticator

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. Reference: https://docs.fortinet.com/document/fortiauthenticator/6.4/administration-guide/372403/fortitoken

NEW QUESTION 44

Why would you configure an OCSP responder URL in an end-entity certificate?
* To provide the CRL location for the certificate
* To identify the end point that a certificate has been assigned to
* To designate the SCEP server to use for CRL updates for that certificate
* To designate a server for certificate status checking

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.

NEW QUESTION 45

Which two statements about the EAP-TTLS authentication method are true? (Choose two)
* Uses mutual authentication
* Uses digital certificates only on the server side
* Requires an EAP server certificate
* Support a port access control (wired) solution only

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. Reference: https://docs.fortinet.com/document/fortiauthenticator/6.4/administration-guide/372412/eap-ttls