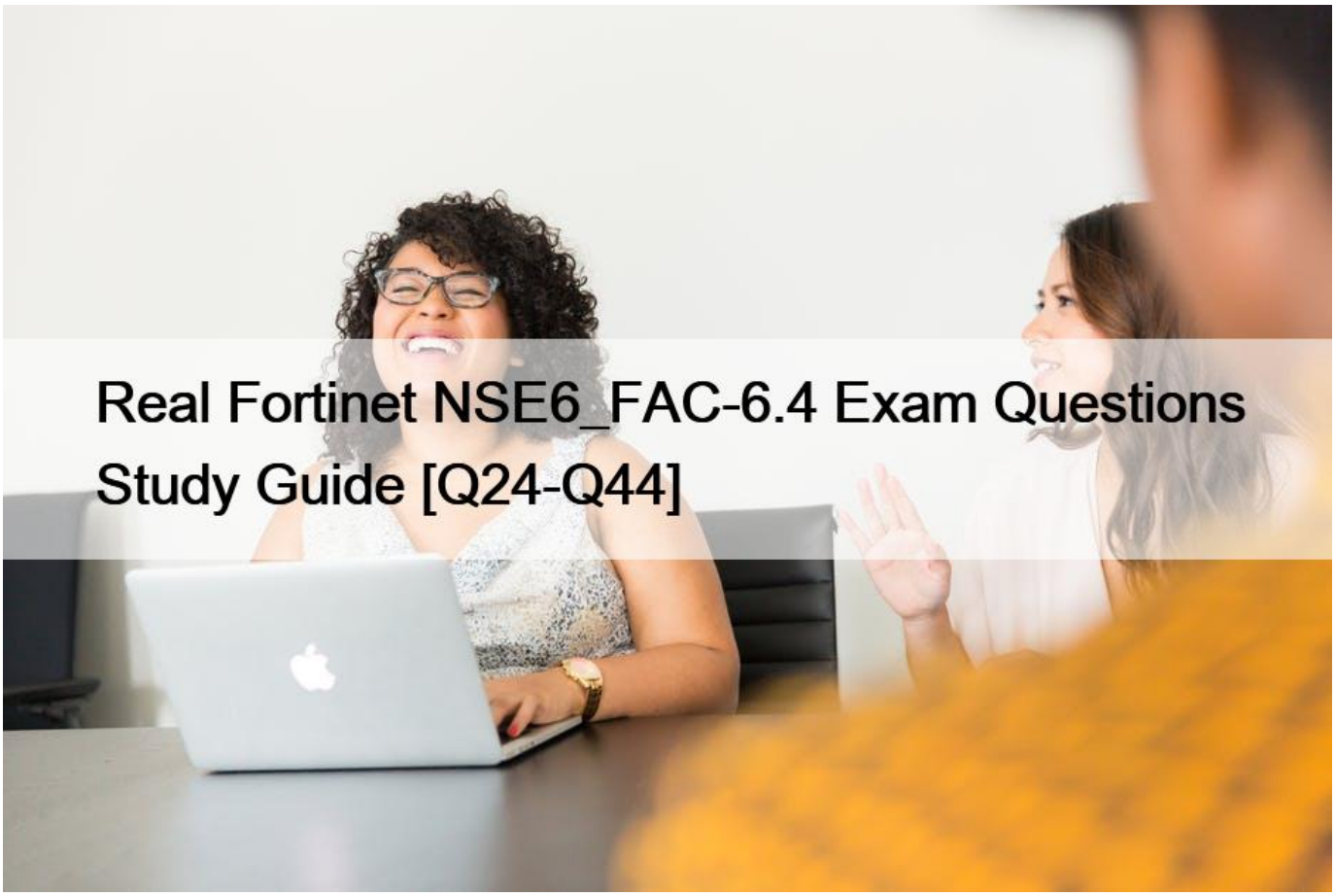
Real Fortinet NSE6_FAC-6.4 Exam Questions Study Guide [Q24-Q44



Real Fortinet NSE6_FAC-6.4 Exam Questions Study Guide
Updated and Accurate NSE6_FAC-6.4 Questions for passing the exam Quickly

NEW QUESTION 24

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 25

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

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 26

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 27

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?

* Create an admin realm in the authentication policy
* Specify the appropriate RADIUS clients in the authentication policy
* Enable Adaptive Authentication in the portal policy
* Enable the Resolve user geolocation from their IP address option in the authentication policy.

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.

NEW QUESTION 28

Which network configuration is required when deploying FortiAuthenticator for portal services?

* FortiAuthenticator must have the REST API access enable on port1
* One of the DNS servers must be a FortiGuard DNS server
* Fortigate must be setup as default gateway for FortiAuthenticator
* Policies must have specific ports open between FortiAuthenticator and the authentication clients

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

NEW QUESTION 29

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?
* FortiToken 200 license has expired
* One of the FortiAuthenticator devices in the active-active cluster has failed
* Time drift between FortiAuthenticator and hardware tokens
* FortiAuthenticator has lost contact with the FortiToken Cloud servers

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.

NEW QUESTION 30

Which two types of digital certificates can you create in Fortiauthenticator? (Choose two)
* User certificate
* Organization validation certificate
* Third-party root certificate
* Local service certificate

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.

NEW QUESTION 31

When generating a TOTP for two-factor authentication, what two pieces of information are used by the algorithm to generate the TOTP?
* UUID and time
* Time and seed
* Time and mobile location
* Time and FortiAuthenticator serial number

TOTP stands for Time-based One-time Password, which is a type of OTP that is generated based on two pieces of information: time

and seed. The time is the current timestamp that is synchronized between the client and the server. The seed is a secret key that is shared between the client and the server. The TOTP algorithm combines the time and the seed to generate a unique and short-lived OTP that can be used for two-factor authentication.

NEW QUESTION 32

Which statement about captive portal policies is true, assuming a single policy has been defined?
* Portal policies apply only to authentication requests coming from unknown RADIUS clients
* All conditions in the policy must match before a user is presented with the captive portal.
* Conditions in the policy apply only to wireless users.
* Portal policies can be used only for BYODs.

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.

NEW QUESTION 33

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 34

Which of the following is an OATH-based standard to generate event-based, one-time password tokens?
* HOTP
* SOTP
* TOTP
* OLTP

Reference:

HOTP stands for HMAC-based One-time Password, which is an OATH-based standard to generate event-based OTP tokens. HOTP uses a cryptographic hash function called HMAC (Hash-based Message Authentication Code) to generate OTPs based on two pieces of information: a secret key and a counter. The counter is incremented by one after each OTP generation, creating an event-based sequence of OTPs.

NEW QUESTION 35

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

NEW QUESTION 36

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?

* By configuring the RADIUS accounting proxy
* By enabling automatic REST API calls from the RADIUS server
* By enabling learning mode in the RADIUS server configuration
* By importing the RADIUS user records

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.

NEW QUESTION 37

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 38

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

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

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. Reference:

https://docs.fortinet.com/document/fortiauthenticator/6.4/administration-guide/372408/certificate-management/372413/certificate-revocation-lists

NEW QUESTION 39

When generating a TOTP for two-factor authentication, what two pieces of information are used by the algorithm to generate the TOTP?
* UUID and time
* Time and FortiAuthenticator serial number
* Time and seed
* Time and mobile location

TOTP stands for Time-based One-time Password, which is a type of OTP that is generated based on two pieces of information: time and seed. The time is the current timestamp that is synchronized between the client and the server. The seed is a secret key that is shared between the client and the server. The TOTP algorithm combines the time and the seed to generate a unique and short-lived OTP that can be used for two-factor authentication.

NEW QUESTION 40

Which two features of FortiAuthenticator are used for EAP deployment? (Choose two)
* Certificate authority
* LDAP server
* MAC authentication bypass
* RADIUS server

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.

NEW QUESTION 41

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 42

When you are setting up two FortiAuthenticator devices in active-passive HA, which HA role must you select on the master FortiAuthenticator?
* Active-passive master
* Standalone master
* Cluster member
* Load balancing master

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