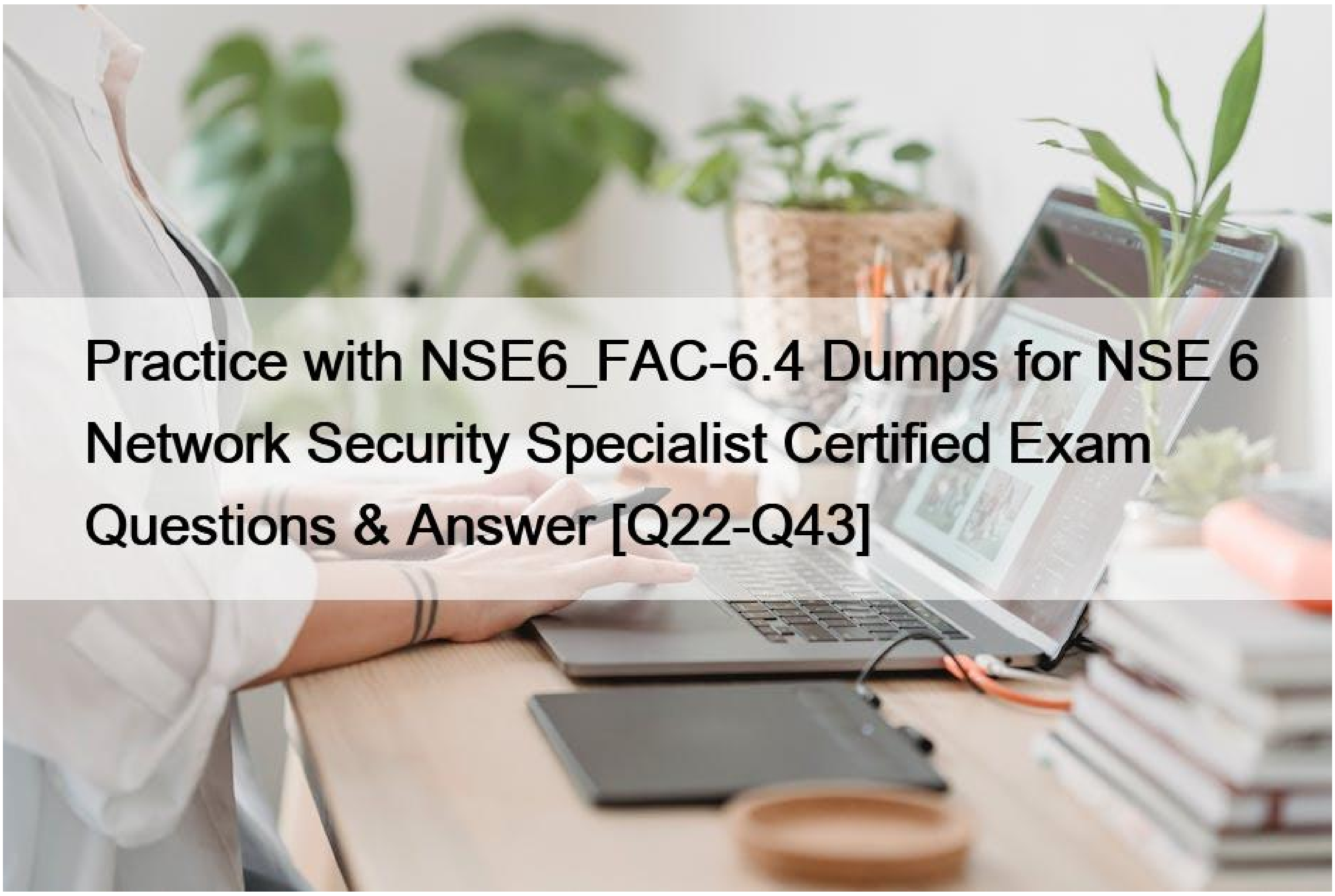
Practice with NSE6_FAC-6.4 Dumps for NSE 6 Network Security Specialist Certified Exam Questions & Answer [Q22-Q43


Practice with NSE6_FAC-6.4 Dumps for NSE 6 Network Security Specialist Certified Exam Questions & Answer [Q22-Q43]

Practice with NSE6_FAC-6.4 Dumps for NSE 6 Network Security Specialist Certified Exam Questions & Answer
REAL NSE6_FAC-6.4 Exam Questions With 100% Refund Guarantee

Fortinet NSE6_FAC-6.4 Exam Syllabus Topics:

TopicDetailsTopic 1- Understand and configure administrative accounts and roles- Configure tokens and two-factor authentication
Topic 2- Use the FortiAuthenticator certificate management service to generate local certificates- Configure and manage user accountsTopic 3- Implement SAML roles on FortiAuthenticator for the SAML SSO service- Configure FortiAuthenticator for deploymentTopic 4- Use local authentication events for Fortinet Single Sign-On (FSSO)- Implement RADIUS profiles and realms for RADIUS authenticationTopic 5- Use FortiAuthenticator portal services to authenticate local and remote users- Configure and manage supported remote authentication servicesTopic 6- Use third-party logon events via RADIUS single sign-on (RSSO), tags, and logs to generate FSSO events- Configure advanced system settings

Fortinet NSE6_FAC-6.4 (Fortinet NSE 6 - FortiAuthenticator 6.4) Certification Exam is a crucial step for anyone seeking to advance their career in network security. NSE6_FAC-6.4 exam tests the individual's knowledge and skills in deploying and managing Fortinet FortiAuthenticator 6.4 solutions. It is designed to certify that an individual possesses the necessary knowledge and skills required to develop and administer a secure user authentication environment.

NEW QUESTION 22

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 23

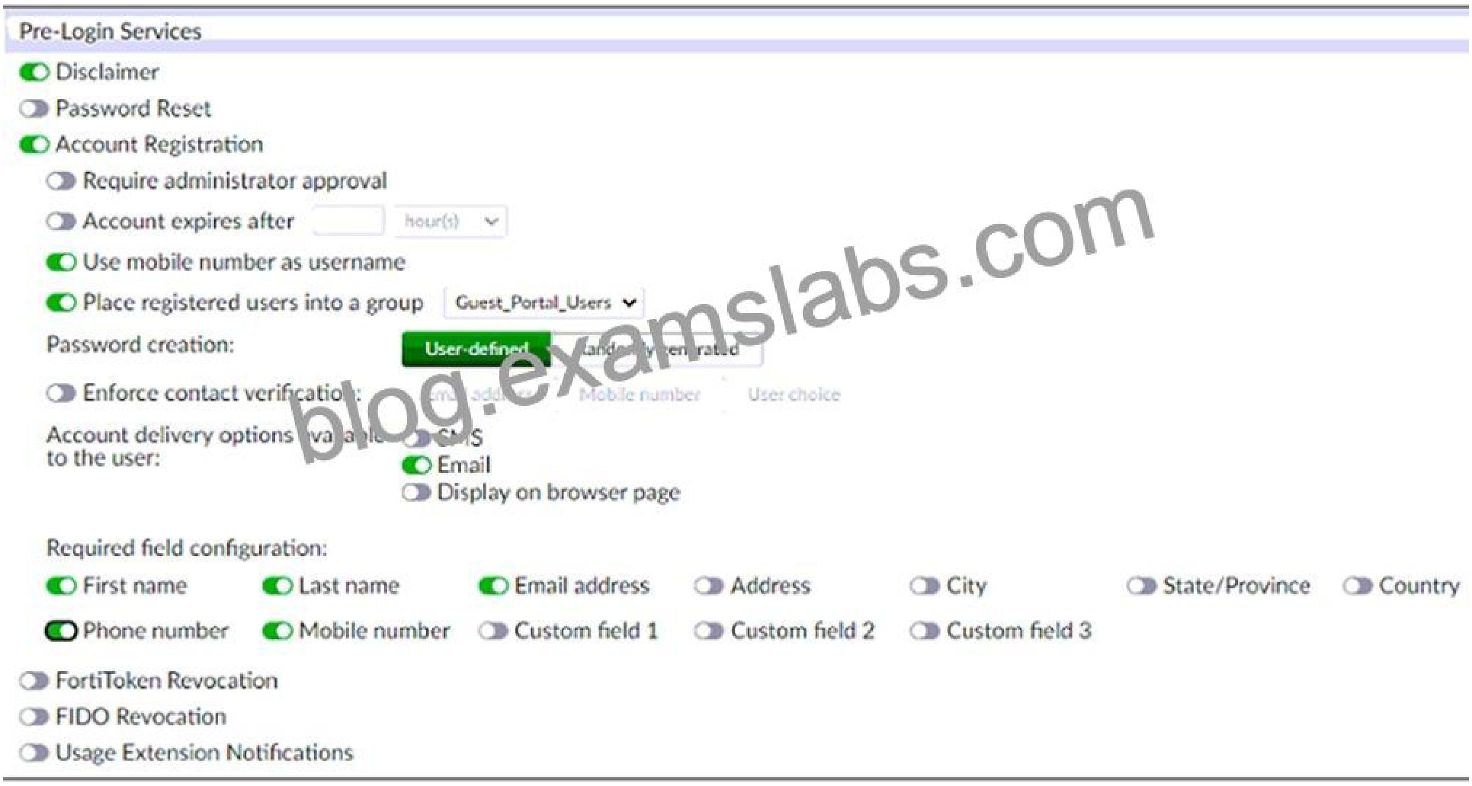
When generating a TOTP for two-factor authentication, what two pieces of information are used by the algorithm to generate the TOTP?
* UUID and time
* Time and seed
* Time and mobile location
* Time and FortiAuthenticator serial number
TOTP stands for Time-based One-time Password, which is a type of 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 24

Which two protocols are the default management access protocols for administrative access for FortiAuthenticator? (Choose two)
* Telnet
* HTTPS
* SSH
* SNMP
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.

NEW QUESTION 25

Examine the screenshot shown in the exhibit.



Pre-Login Services

● Disclaimer

○ Password Reset

● Account Registration

- ○ Require administrator approval
- ○ Account expires after [ ] hour(s)
- ● Use mobile number as username
- ● Place registered users into a group Guest_Portal_Users
- Password creation: [✓ User-defined] Randomly generated
- ○ Enforce contact verification: Email address / Mobile number / User choice
- Account delivery options available to the user: ○ SMS ● Email ○ Display on browser page
- Required field configuration: ● First name ● Last name ● Email address ○ Address ○ City ○ State/Province ○ Country ● Phone number ● Mobile number ○ Custom field 1 ○ Custom field 2 ○ Custom field 3

○ FortiToken Revocation

○ FIDO Revocation

○ Usage Extension Notifications

Which two statements regarding the configuration are true? (Choose two.)

* All guest accounts created using the account registration feature will be placed under the Guest_Portal_Users group
* All accounts registered through the guest portal must be validated through email
* Guest users must fill in all the fields on the registration form
* Guest user account will expire after eight hours

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.

NEW QUESTION 26

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

* Windows AD polling
* FortiClient SSO Mobility Agent
* Radius Accounting
* DC Polling

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.

NEW QUESTION 27

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 28

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

* Enable syslog on the FortiAuthenticator interface.
* Define a syslog source.
* Select a syslog rule for message parsing.
* Set the same password on both the FortiAuthenticator and the syslog server.
* Set the syslog UDP port on FortiAuthenticator.

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.

NEW QUESTION 29

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 30

Which three of the following can be used as SSO sources? (Choose three)

* FortiClient SSO Mobility Agent
* SSH Sessions
* FortiAuthenticator in SAML SP role
* Fortigate
* RADIUS accounting

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. Reference:
https://docs.fortinet.com/document/fortiauthenticator/6.4/administration-guide/372410/single-sign-on

NEW QUESTION 31

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 32

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 33

What capability does the inbound proxy setting provide?
* It allows FortiAuthenticator to determine the origin source IP address after traffic passes through a proxy for system access,
* It allows FortiAuthenticator to act as a proxy for remote authentication servers.
* It allows FortiAuthenticator the ability to round robin load balance remote authentication servers.
* It allows FortiAuthenticator system access to authenticating users, based on a geo IP address designation.
The inbound proxy setting provides the ability for FortiAuthenticator to determine the origin source IP address after traffic passes through a proxy for system access. The inbound proxy setting allows FortiAuthenticator to use the X-Forwarded-For header in the

HTTP request to identify the original client IP address. This can help FortiAuthenticator apply the correct authentication policy or portal policy based on the source IP address.

NEW QUESTION 34

An administrator has an active directory (AD) server integrated with FortiAuthenticator. They want members of only specific AD groups to participate in FSSO with their corporate FortiGate firewalls.

How does the administrator accomplish this goal?
* Configure a FortiGate filter on FortiAuthenticatoc
* Configure a domain groupings list to identify the desired AD groups.
* Configure fine-grained controls on FortiAuthenticator to designate AD groups.
* Configure SSO groups and assign them to FortiGate groups.
To allow members of only specific AD groups to participate in FSSO with their corporate FortiGate firewalls, the administrator can configure SSO groups and assign them to FortiGate groups. SSO groups are groups of users or devices that are defined on FortiAuthenticator based on various criteria, such as user group membership, source IP address, MAC address, or device type. FortiGate groups are groups of users or devices that are defined on FortiGate based on various criteria, such as user group membership, firewall policy, or authentication method. By mapping SSO groups to FortiGate groups, the administrator can control which users or devices can access the network resources protected by FortiGate.

NEW QUESTION 35

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 36

Which EAP method is known as the outer authentication method?
* PEAP
* EAP-GTC
* EAP-TLS
* MSCHAPV2
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.

NEW QUESTION 37

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 38

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 39

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 40

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

* To designate the SCEP server to use for CRL updates for that certificate
* To identify the end point that a certificate has been assigned to
* To designate a server for certificate status checking
* To provide the CRL location for the certificate

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.

PDF Download Fortinet Test To Gain Brilliante Result!: https://www.examslabs.com/Fortinet/NSE-6-Network-Security-Specialist/best-NSE6_FAC-6.4-exam-dumps.html]