Fortinet

Exam Questions NSE6_FAC-6.4

Fortinet NSE 6 - FortiAuthenticator 6.4

NEW QUESTION 1
At a minimum, which two configurations are required to enable guest portal services on FortiAuthenticator? (Choose two)

A. Configuring a portal policy
B. Configuring at least on post-login service
C. Configuring a RADIUS client
D. Configuring an external authentication portal

Answer: AB

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

NEW QUESTION 2
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 3
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 4
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 5
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 6
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 7
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?

A. Configure a FortiGate filter on FortiAuthenticatoc
B. Configure a domain groupings list to identify the desired AD groups.
C. Configure fine-grained controls on FortiAuthenticator to designate AD groups.
D. Configure SSO groups and assign them to FortiGate groups.

Answer: D

Explanation:
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.
References:
https://docs.fortinet.com/document/fortiauthenticator/6.4.0/administration-guide/906179/single-sign-on#sso-gro

NEW QUESTION 8
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 9
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 10
Which two statements about the EAP-TTLS authentication method are true? (Choose two)

A. Uses mutual authentication
B. Uses digital certificates only on the server side
C. Requires an EAP server certificate
D. Support a port access control (wired) solution only

Answer: BC

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

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 11
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 13
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 14
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 16
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 21
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 23
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 27
When generating a TOTP for two-factor authentication, what two pieces of information are used by the algorithm to generate the TOTP?

A. UUID and time
B. Time and seed
C. Time and mobile location
D. Time and FortiAuthenticator serial number

Answer: B

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

NEW QUESTION 32
......