Fortinet.NSE6_FAC-6.4.vJun-2024.by.Waren.32q

Number: NSE6_FAC-6.4
Passing Score: 800
Time Limit: 120
File Version: 4.0

Exam Code: NSE6_FAC-6.4

Exam Name: Fortinet NSE 6 - FortiAuthenticator 6.4

Exam A

QUESTION 1
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 balancers B 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

Correct Answer: B
Section:
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
Reference: https://docs.fortinet.com/document/fortiauthenticator/6.4.0/administrationguide/ 906179/high-availability#ha-and-load-balancing

QUESTION 2
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.

Correct Answer: D
Section:
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.
Reference: https://docs.fortinet.com/document/fortiauthenticator/6.4.0/administrationguide/ 906179/single-sign-on#sso-groups

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

Correct Answer: B

Section:
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.
Reference: https://docs.fortinet.com/document/fortiauthenticator/6.4.0/administrationguide/ 906179/single-sign-on#forticlient-sso-mobility-agent

QUESTION 4
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

Correct Answer: B
Section:
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.
Reference: https://docs.fortinet.com/document/fortiauthenticator/6.4.0/administrationguide/ 906179/two-factor-authentication#totp

QUESTION 5
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

Correct Answer: A
Section:
Explanation:
Reference: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortitoken.pdf 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 eventbased sequence of OTPs.
Reference: https://docs.fortinet.com/document/fortiauthenticator/6.4.0/administrationguide/ 906179/two-factor-authentication#hotp

QUESTION 6
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?

A. Create realms.
B. Create user groups
C. Create multiple directory trees on FortiAuthenticator
D. Automatically import hosts from each domain as they authenticate.

Correct Answer: A

Section:
Explanation:
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.
Reference: https://docs.fortinet.com/document/fortiauthenticator/6.4.0/administrationguide/ 906179/user-management#realms

QUESTION 7
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.

Correct Answer: C
Section:
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.
Reference: https://docs.fortinet.com/document/fortiauthenticator/6.4.0/administrationguide/ 906179/authentication-policies#adaptive-authentication

QUESTION 8
Which network configuration is required when deploying FortiAuthenticator for portal services?

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

Correct Answer: D
Section:
Explanation:
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 Reference:
https://docs.fortinet.com/document/fortiauthenticator/6.4.0/administrationguide/ 906179/portal-services#network-configuration

QUESTION 9
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?

A. FortiToken 200 license has expired
B. One of the FortiAuthenticator devices in the active-active cluster has failed
C. Time drift between FortiAuthenticator and hardware tokens
D. FortiAuthenticator has lost contact with the FortiToken Cloud servers

Correct Answer: C
Section:
Explanation:
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.
Reference: https://docs.fortinet.com/document/fortiauthenticator/6.4.0/administrationguide/ 906179/two-factor-authentication#time-drift-tolerance

QUESTION 10
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

Correct Answer: C
Section:
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.
Reference: https://docs.fortinet.com/document/fortiauthenticator/6.4.0/administrationguide/ 906179/certificate-management#ocsp-responder

QUESTION 11
An administrator wants to keep local CA cryptographic keys stored in a central location.
Which FortiAuthenticator feature would provide this functionality?

A. SCEP support
B. REST API
C. Network HSM
D. SFTP server

Correct Answer: C
Section:
Explanation:
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.
Reference: https://docs.fortinet.com/document/fortiauthenticator/6.4.0/administrationguide/ 906179/certificate-management#network-hsm

QUESTION 12
Which option correctly describes an SP-initiated SSO SAML packet flow for a host without a SAML assertion?

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

Correct Answer: C
Section:
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.
Reference: https://docs.fortinet.com/document/fortiauthenticator/6.4.0/administrationguide/ 906179/saml-service-provider#sp-initiated-sso

QUESTION 13
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

Correct Answer: A, D
Section:
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.
Reference: https://docs.fortinet.com/document/fortiauthenticator/6.4.0/administrationguide/ 906179/certificate-management#certificate-types

QUESTION 14
Which EAP method is known as the outer authentication method?

A. PEAP
B. EAP-GTC
C. EAP-TLS
D. MSCHAPV2

Correct Answer: A
Section:
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.
Reference: https://docs.fortinet.com/document/fortiauthenticator/6.4.0/administrationguide/ 906179/wireless-802-1x-authentication#peap

QUESTION 15
You want to monitor FortiAuthenticator system information and receive FortiAuthenticator traps through SNMP.
Which two configurations must be performed after enabling SNMP access on the FortiAuthenticator interface? (Choose two)

A. Enable logging services
B. Set the tresholds to trigger SNMP traps
C. Upload management information base (MIB) files to SNMP server

D. Associate an ASN, 1 mapping rule to the receiving host

Correct Answer: B, C
Section:
Explanation:
To monitor FortiAuthenticator system information and receive FortiAuthenticator traps through SNMP, two configurations must be performed after enabling SNMP access on the FortiAuthenticator interface:
Set the thresholds to trigger SNMP traps for various system events, such as CPU usage, disk usage, memory usage, or temperature.
Upload management information base (MIB) files to SNMP server to enable the server to interpret the SNMP traps sent by FortiAuthenticator.
Reference: https://docs.fortinet.com/document/fortiauthenticator/6.4.0/administrationguide/ 906179/system-settings#snmp

QUESTION 16
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

Correct Answer: A, D
Section:
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.
Reference: https://docs.fortinet.com/document/fortiauthenticator/6.4.0/administrationguide/ 906179/wireless-802-1x-authentication

QUESTION 17
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

Correct Answer: B
Section:
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.
Reference: https://docs.fortinet.com/document/fortiauthenticator/6.4.0/administrationguide/ 906179/saml-service-provider#saml-metadata

QUESTION 18
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

Correct Answer: C
Section:
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.
Reference: https://docs.fortinet.com/document/fortiauthenticator/6.4.0/administrationguide/ 906179/rest-api

QUESTION 19
Which statement about captive portal policies is true, assuming a single policy has been defined?

A. Portal policies apply only to authentication requests coming from unknown RADIUS clients

B. All conditions in the policy must match before a user is presented with the captive portal.

C. Conditions in the policy apply only to wireless users.

D. Portal policies can be used only for BYODs.

Correct Answer: B
Section:
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.
Reference: https://docs.fortinet.com/document/fortiauthenticator/6.4.0/administrationguide/ 906179/portal-services#captive-portal-policies

QUESTION 20
Which interface services must be enabled for the SCEP client to connect to Authenticator?

A. OCSP

B. REST API

C. SSH

D. HTTP/HTTPS

Correct Answer: D
Section:
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.
Reference: https://docs.fortinet.com/document/fortiauthenticator/6.4.0/administrationguide/ 906179/certificate-management#scep

QUESTION 21
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.

Correct Answer: D
Section:
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.
Reference: https://docs.fortinet.com/document/fortiauthenticator/6.4.0/administrationguide/ 906179/administrators#admin-profiles

QUESTION 22
Which two protocols are the default management access protocols for administrative access for FortiAuthenticator? (Choose two)

A. Telnet

B. HTTPS

C. SSH

D. SNMP

Correct Answer: B, C
Section:
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.
Reference: https://docs.fortinet.com/document/fortiauthenticator/6.4.0/administration-guide/906179/system-settings#management-access

QUESTION 23
When configuring syslog SSO, which three actions must you take, in addition to enabling the syslog SSO method? (Choose three.)

A. Enable syslog on the FortiAuthenticator interface.

B. Define a syslog source.

C. Select a syslog rule for message parsing.

D. Set the same password on both the FortiAuthenticator and the syslog server.

E. Set the syslog UDP port on FortiAuthenticator.

Correct Answer: B, C, E
Section:
Explanation:
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.
Reference: https://docs.fortinet.com/document/fortiauthenticator/6.4.0/administrationguide/ 906179/single-sign-on#syslog-sso

QUESTION 24
What capability does the inbound proxy setting provide?

A. It allows FortiAuthenticator to determine the origin source IP address after traffic passes through a proxy for system access,

B. It allows FortiAuthenticator to act as a proxy for remote authentication servers.

C. It allows FortiAuthenticator the ability to round robin load balance remote authentication servers.

D. It allows FortiAuthenticator system access to authenticating users, based on a geo IP address designation.

Correct Answer: A
Section:
Explanation:
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.
Reference: https://docs.fortinet.com/document/fortiauthenticator/6.4.0/administrationguide/ 906179/system-settings#inbound-proxy

QUESTION 25
Which two SAML roles can Fortiauthenticator be configured as? (Choose two)

A. Idendity provider

B. Principal

C. Assertion server

D. Service provider

Correct Answer: A, D
Section:
Explanation:
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

QUESTION 26
What happens when a certificate is revoked? (Choose two)

A. Revoked certificates cannot be reinstated for any reason

B. All certificates signed by a revoked CA certificate are automatically revoked

C. Revoked certificates are automatically added to the CRL

D. External CAs will priodically query Fortiauthenticator and automatically download revoked certificates

Correct Answer: B, C
Section:
Explanation:
When a certificate is revoked, it means that it is no longer valid and should not be trusted by any entity. Revoked certificates are automatically added to the certificate revocation list (CRL) which is published by the issuing CA and can be checked by other parties. If a CA certificate is revoked, all certificates signed by that CA are also revoked and added to the CRL. Revoked certificates can be reinstated if the reason for revocation is resolved, such as a compromised private key being recovered or a misissued certificate being corrected. External CAs do not query FortiAuthenticator for revoked certificates, but they can use protocols such as SCEP or OCSP to exchange certificate information with FortiAuthenticator. Reference: https://docs.fortinet.com/document/fortiauthenticator/6.4/administrationguide/ 372408/certificate-management

QUESTION 27
You are the administrator of a large network that includes a large local user datadabase on the current Fortiauthenticatior. You want to import all the local users into a new Fortiauthenticator device.
Which method should you use to migrate the local users?

A. Import users using RADIUS accounting updates.

B. Import the current directory structure.

C. Import users from RADUIS.

D. Import users using a CSV file.

Correct Answer: D
Section:
Explanation:
The best method to migrate local users from one FortiAuthenticator device to another is to export the users from the current device as a CSV file and then import the CSV file into the new device. This method preserves all the user attributes and settings and allows you to modify them if needed before importing. The other methods are not suitable for migrating local users because they either require an external RADIUS server or do not transfer all the user information. Reference: https://docs.fortinet.com/document/fortiauthenticator/6.4/administration-guide/372409/usermanagement

QUESTION 28
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

Correct Answer: A, D, E
Section:
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. Reference:
https://docs.fortinet.com/document/fortiauthenticator/6.4/administration-guide/372410/singlesign-on

QUESTION 29
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

Correct Answer: B, D
Section:
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. Reference: https://docs.fortinet.com/document/fortiauthenticator/6.4/administrationguide/ 372408/certificate-management

QUESTION 30
Which statement about the guest portal policies is true?

A. Guest portal policies apply only to authentication requests coming from unknown RADIUS clients
B. Guest portal policies can be used only for BYODs
C. Conditions in the policy apply only to guest wireless users
D. All conditions in the policy must match before a user is presented with the guest portal

Correct Answer: D
Section:
Explanation:
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/guestmanagement/ 372406/portal-policies

QUESTION 31
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

Correct Answer: A
Section:
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). Reference: https://docs.fortinet.com/document/fortiauthenticator/6.4/administrationguide/ 372411/high-availability

QUESTION 32
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

Correct Answer: B, C
Section:
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. Reference: https://docs.fortinet.com/document/fortiauthenticator/6.4/administration-guide/372412/eap-ttls