Fortinet.Pre.NSE6_FAC-6.1 .30q - DEMO

Number: NSE6_FAC-6.1
Passing Score: 800
Time Limit: 120 min
File Version: 1.0

Exam Code: NSE6_FAC-6.1
Exam Name: Fortinet NSE 6 - FortiAuthenticator 6.1
Website: https://VCEup.com/

QUESTION 1
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: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 2
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: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 3
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: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 4
Which two are supported captive or guest portal authentication methods? (Choose two)

A. LinkedIn
B. Apple ID
C. Instagram
D. Email

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 5
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: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 6
A device or user identity cannot be established transparently, such as with non-domain BYOD devices, and allow users to create their own credentialis.
In this case, which user idendity discovery method can Fortiauthenticator use?

A. Syslog messaging or SAML IDP
B. Kerberos-base authentication
C. Radius accounting
D. Portal authentication

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 7
Which two SAML roles can Fortiauthenticator be configured as? (Choose two)

A. Idendity provider
B. Principal
C. Assertion server
D. Service provider

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 8
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: CD
Section: (none)

Explanation

Explanation/Reference:
Explanation:

QUESTION 9
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: AD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 10
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: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 11
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: ACE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 12
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: BD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 13
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: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 14
Refer to the exhibit.

Examine the screenshot shown in the exhibit.
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

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 15
Which EAP method is known as the outer authentication method?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 16
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: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 17
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: BC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 18
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 couse this issue?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 19
Which behaviors exist for certificate revocation lists (CRLs) on FortiAuthenticator? (Choose two)

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

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 20
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: AD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

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

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 22
Which of the following is an QATH-based standart to generate event-based, one-time password tokens?

A. OLTP
B. SOTP
C. HOTP
D. TOTP

Correct Answer: C
Section: (none)

Explanation

Explanation/Reference:
Explanation:

QUESTION 23
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. Automatically import hosts from each domain as they authenticate
B. Create multiple directory trees on FortiAuthenticator
C. Create realms
D. Create user groups

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 24
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: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 25
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

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 26
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: BC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 27
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 28
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: BC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 29
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

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 30
Which two statement about the RADIUS service on FortiAuthenticator are true? (Choose two)

A. Two-factor authentication cannot be enforced when using RADIUS authentication
B. RADIUS users can migrated to LDAP users
C. Only local users can be authenticated through RADIUS

D. FortiAuthenticator answers only to RADIUS client that are registered with FortiAuthenticator

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Explanation: