Free Questions for NSE6_FAC-6.4 by dumpshq

Shared by Coleman on 07-06-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

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

Options:

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:

A, B

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

Question 2

Question Type: **MultipleChoice**

Which method is the most secure way of delivering FortiToken data once the token has been seeded?

Options:

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. Reference: https://docs.fortinet.com/document/fortiauthenticator/6.4/administration-guide/372403/fortitoken

Question 3

Question Type: MultipleChoice

What are three key features of FortiAuthenticator? (Choose three)

Options:

A- Identity management device

B- Log server

C- Certificate authority

D- Portal services

E- RSSO Server

Answer:

A, C, D

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.
Reference: https://docs.fortinet.com/document/fortiauthenticator/6.4/release-notes

Question 4

Question Type: MultipleChoice

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

Options:

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

Answer:

A, B

Explanation:

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

Question 5

Question Type: MultipleChoice

Which two statements about the EAP-TTLS authentication method are true? (Choose two)

Options:

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:

B, C

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

Question 6

Question Type: MultipleChoice

Which two statements about the EAP-TTLS authentication method are true? (Choose two)

Options:

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:

B, C

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

Question 7

Question Type: MultipleChoice

Which method is the most secure way of delivering FortiToken data once the token has been seeded?

Options:

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. Reference: https://docs.fortinet.com/document/fortiauthenticator/6.4/administration-guide/372403/fortitoken

Question 8

Question Type: MultipleChoice

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

Options:

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

Answer:

A, B

Explanation:

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

Question 9

Question Type: MultipleChoice

What are three key features of FortiAuthenticator? (Choose three)

Options:

A- Identity management device

B- Log server

C- Certificate authority

D- Portal services

E- RSSO Server

Answer:

A, C, D

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.
Reference: https://docs.fortinet.com/document/fortiauthenticator/6.4/release-notes

Question 10

Question Type: MultipleChoice

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

Options:

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:

A, B

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