NSE6_FAC-6.1^{Q&As}

Fortinet NSE 6 - FortiAuthenticator 6.1

Pass Fortinet NSE6_FAC-6.1 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/nse6_fac-6-1.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Fortinet Official Exam Center

QUESTION 1

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

QUESTION 2

A device or useridentity 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

QUESTION 3

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

QUESTION 4

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 serviceprovider, 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

QUESTION 5

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

Latest NSE6_FAC-6.1 Dumps   NSE6_FAC-6.1 Study Guide   NSE6_FAC-6.1 Exam Questions