NSE7_SAC-6.2 Q&As

Fortinet NSE 7 - Secure Access 6.2

Pass Fortinet NSE7_SAC-6.2 Exam with 100% Guarantee

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

https://www.pass4itsure.com/nse7_sac-6-2.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

What is the purpose of configuring the Windows Active Directory Domain Authentication feature?

A. Allows FortiAuthenticator to register itself as a Windows trusted device to proxy CHAP authentication using Kerberos.

B. Allows FortiAuthenticator to use Windows administrator credentials to perform an LDAP lookup for a user search.

C. Allows FortiAuthenticator to use a Windows CA certificate when authenticating RADIUS users.

D. Allows FortiAuthenticator to authenticate users listed on Windows AD. Enables single sign-on services for VPN and wireless users.

Correct Answer: D

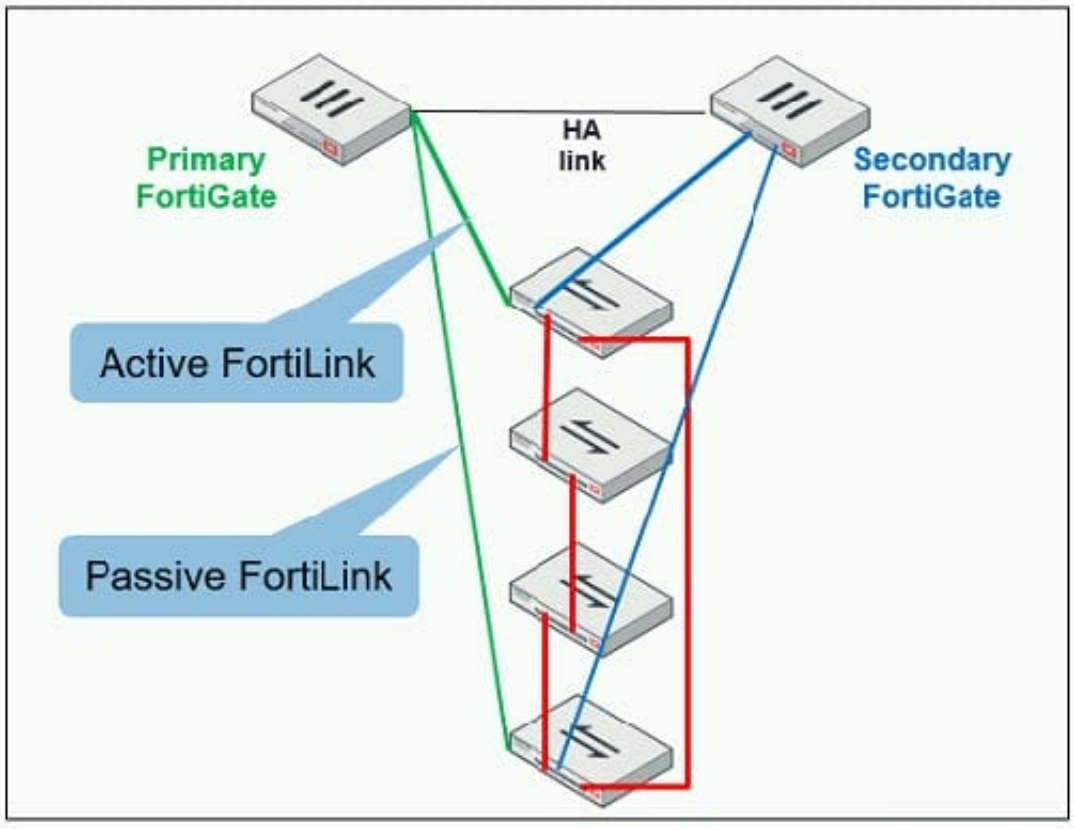
Reference: https://docs.fortinet.com/document/fortiauthenticator/6.0.0/administration-guide/641286/ remote-authentication-servers

QUESTION 2

Refer to the exhibit.

The exhibit shows two FortiGate devices in active-passive HA mode, including four FortiSwitch devices

connected to a ring.



Which two configurations are required to deploy this network topology? (Choose two.)

A. Configure link aggregation interfaces on the FortiLink interfaces.

B. Configure the trunk interfaces on the FortiSwitch devices as MCLAG-ISL.

C. Enable fortilink-split-interfaceon the FortiLink interfaces.

D. Enable STP on the FortiGate interfaces.

Correct Answer: CD

Reference: https://www.fortinetguru.com/2019/07/fortilink-configuration-using-the-fortigate-gui/

QUESTION 3

Examine the sections of the configuration shown in the following output:

```
config vpn certificate setting
    set ocsp-status enable
    set ocsp-default-server "FAC"
    set strict-ocsp-check disable
end
config vpn certificate ocsp-server
    edit "FAC"
        set url "http://10.0.1.150:2560"
        set unavail-action revoke
    next
end
config vpn ssl settings
   set ssl-ocsp-option certificate
end
```

What action will the FortiGate take when using OCSP certificate validation?

A. FortiGate will reject the certificate if the OCSP server replies that the certificate is unknown.

B. FortiGate will use the OCSP server 10.0.1.150 even when the OCSP URL field in the user certificate

contains a different OCSP server IP address.

C. FortiGate will use the OCSP server 10.0.1.150 even when there is a different OCSP IP address in the ocsp-override-serveroption under config user peer.

D. FortiGate will invalidate the certificate if the OSCP server is unavailable.

Correct Answer: D

QUESTION 4

Which two EAP methods can use MSCHAPV2 for client authentication? (Choose two.)

A. PEAP

B. EAP-TTLS

C. EAP-TLS

D. EAP-GTC

Correct Answer: AC

Reference: https://help.fortinet.com/fauth/3-3/Content/FortiAuthenticator%203_3%20Admin%20Guide/500/501_EAP.htm

QUESTION 5

Refer to the exhibit.

```
FortiGate # diagnose switch-controller switch-info 802.1X
Managed Switch : S224EPTF18001736

   port2 : Mode: port-based (mac-by-pass disable)
           Link: Link up
           Port State: unauthorized: (  )
           Dynamic Authorized Vlan : 0
           EAP pass-through mode : Enable
           Quarantine VLAN (4093) detection : Enable
           Native Vlan : 10
           Allowed Vlan list: 10,4093
           Untagged Vlan list: 4093
           Guest VLAN :
           Auth-Fail Vlan :

           Sessions info:
           00:09:0f:02:02:02     Type=802.1x,,state=AUTHENTICATING,etime=0,eap_cnt=0 params:reAuth=3600
```

A host machine connected to port2 on FortiSwitch cannot connect to the network. All ports on FortiSwitch are assigned a security policy to enforce 802.1X port authentication. While troubleshooting the issue, the administrator runs the debug command and obtains the output shown in the exhibit.

Which two scenarios are the likely cause of this issue? (Choose two.)

A. The host machine is not configured for 802.1X port authentication.

B. The host machine does not support 802. 1X authentication.

C. The host machine is quarantined due to a security incident.

D. The host machine is configured with wrong VLAN ID.

Correct Answer: AB

Reference: https://kb.fortinet.com/kb/documentLink.do?externalID=FD46428