DUMPSBOSS.

Fortinet NSE 7 - Secure Access 6.2

Fortinet NSE7_SAC-6.2

Version Demo

Total Demo Questions: 5

Total Premium Questions: 30

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

QUESTION NO: 1

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

A. PEAP

B. EAP-TTLS

C. EAP-TLS

D. EAP-GTC

ANSWER: A C

Explanation:

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

QUESTION NO: 2

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.

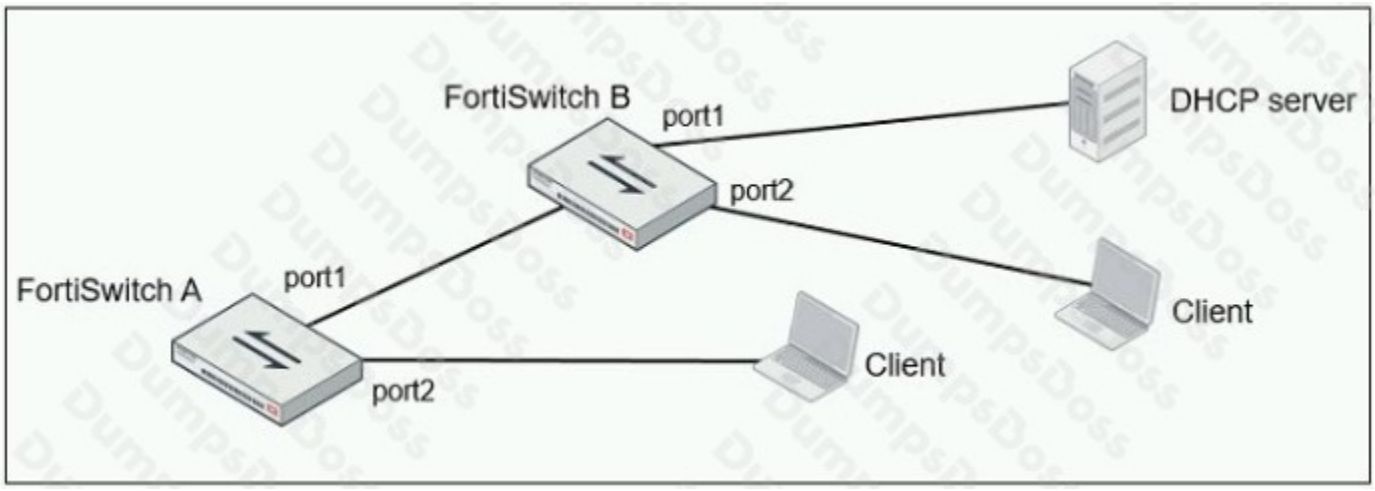
C. FortiGate will use the OCSP server 10.0.1.150 even when there is a different OCSP IP address in the ocsp-override-server option under config user peer.

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

ANSWER: D

QUESTION NO: 3

Refer to the exhibit.



Given the network topology shown in the exhibit, which two ports should be configured as untrusted DHCP ports? (Choose two.)

A. FortiSwitch A, port2

B. FortiSwitch A, port1

C. FortiSwitch B, port1

D. FortiSwitch B, port2

ANSWER: C D

QUESTION NO: 4

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 AEnables single sign-on services for VPN and wireless users.

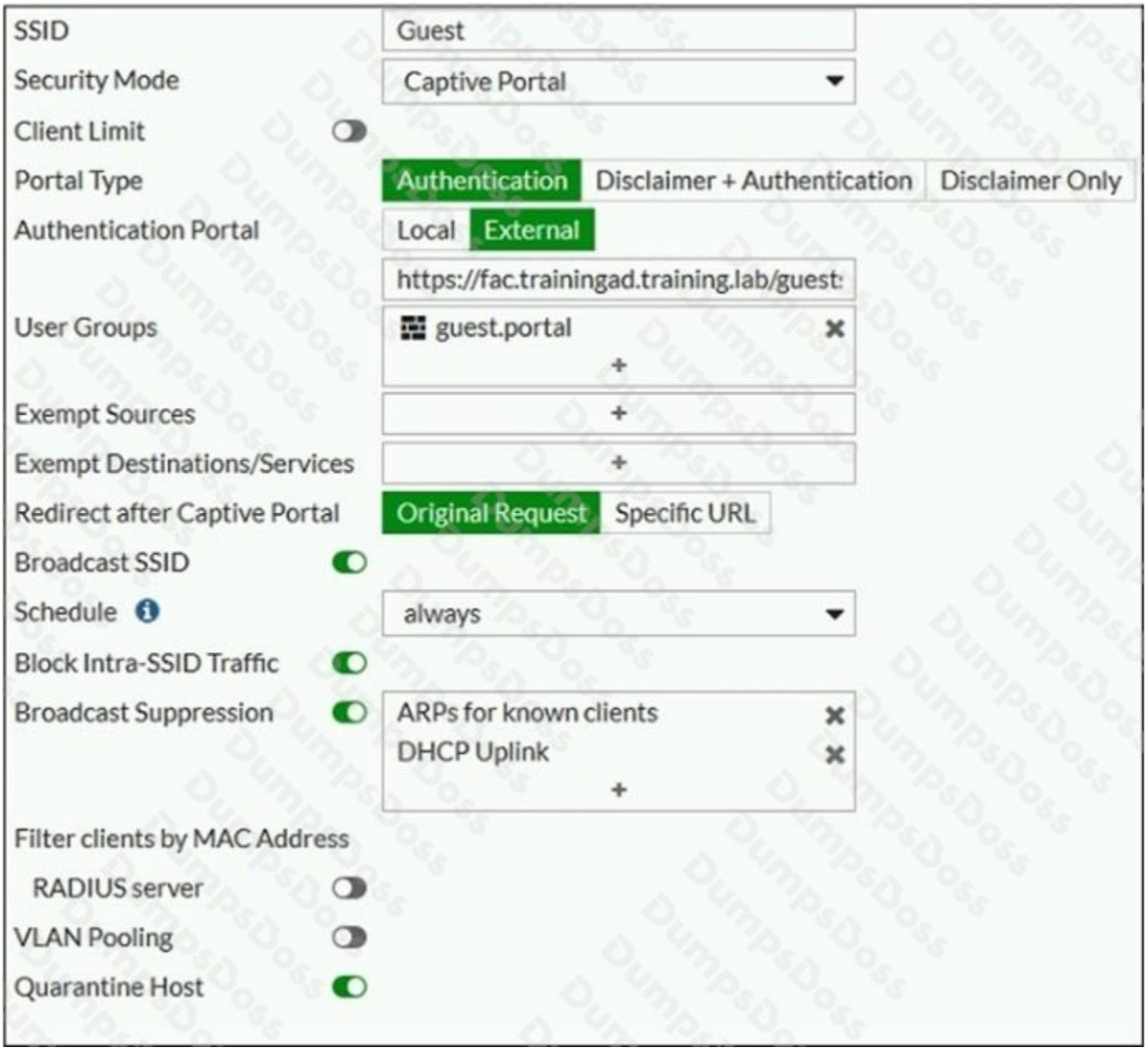
ANSWER: D

Explanation:

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

QUESTION NO: 5

Refer to the exhibits.



Examine the firewall policy configuration and SSID settings.

```
config firewall policy
   edit 11
      set name "Guest to Internal"
      set uuid c5e45130-aada-51e8-ee0c-bc1204f9f163
      set srcintf "guest"
      set dstintf "port3"
      set srcaddr "all"
      set dstaddr: "FortiAuthenticator" "WindowsAD"
      set action accept
      set schedule "always"
      set service "ALL"
   next
end
```

An administrator has configured a guest wireless network on FortiGate using the external captive portal. The administrator has verified that the external captive portal URL is correct. However, wireless users are not able to see the captive portal login page.

Given the configuration shown in the exhibit and the SSID settings, which configuration change should the administrator make to fix the problem?

A. Enable the captive-portal-exempt option in the firewall policy with the ID 11.

B. Apply a guest.portal user group in the firewall policy with the ID 11.

C. Disable the user group from the SSID configuration.

D. Include the wireless client subnet range in the Exempt Source section.

ANSWER: C