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:

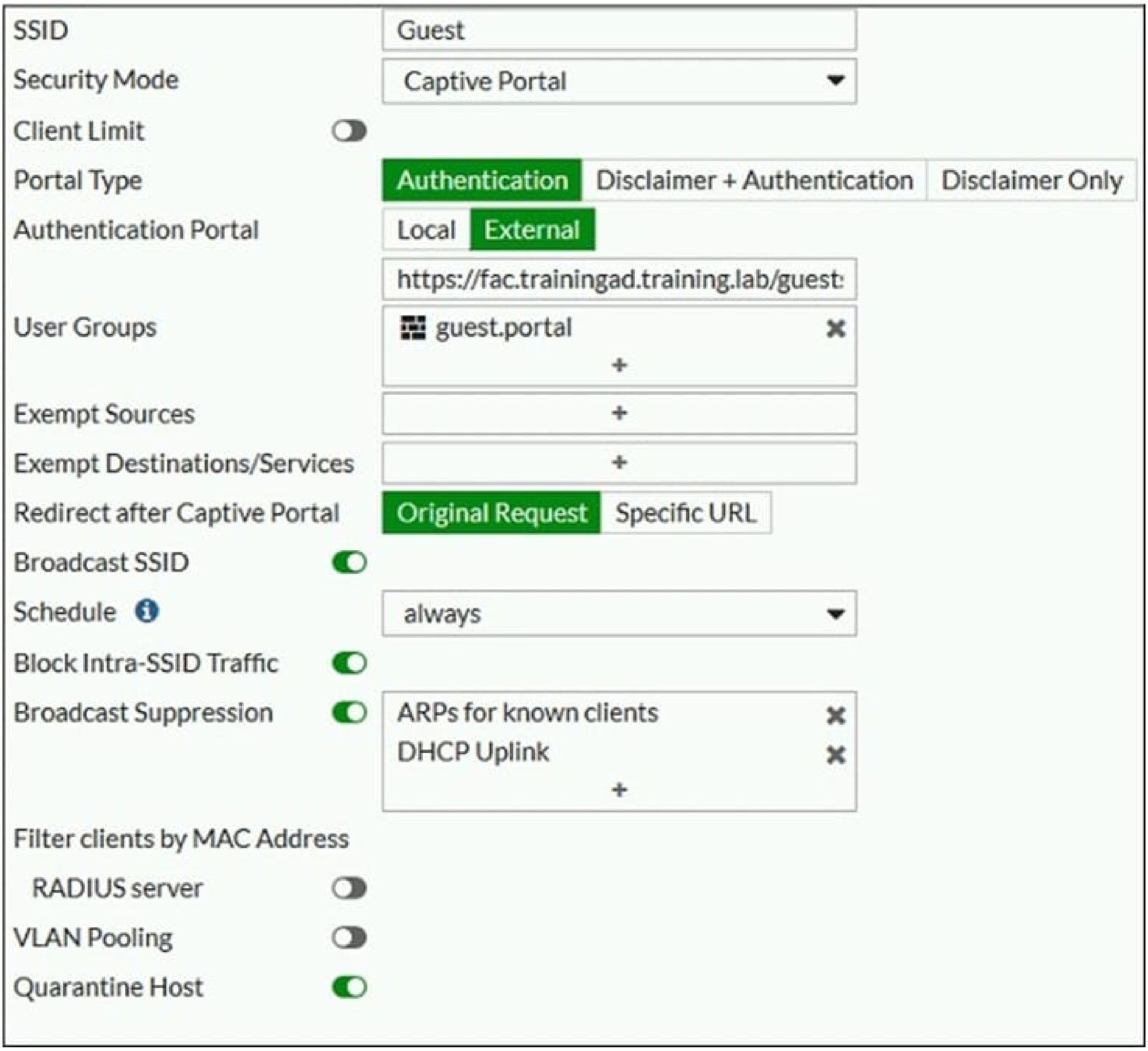
https://www.geekcert.com/nse7_sac-6-2.html

100% Passing Guarantee
100% Money Back Assurance

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

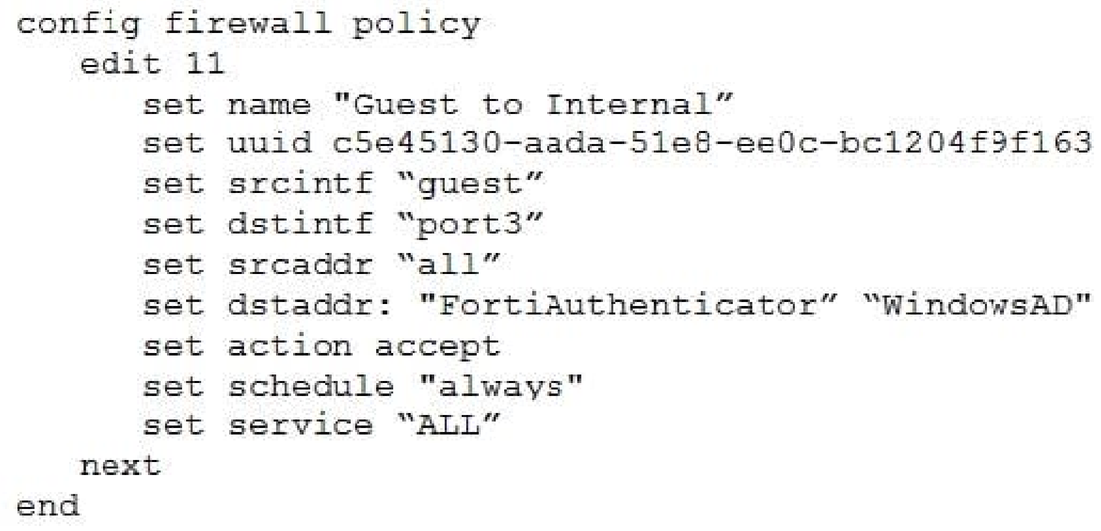
QUESTION 1

Refer to the exhibits.



SSID	Guest
Security Mode	Captive Portal
Client Limit	○
Portal Type	[✓ Authentication] Disclaimer + Authentication Disclaimer Only
Authentication Portal	Local [✓ External]
	https://fac.trainingad.training.lab/guest:
User Groups	guest.portal ✖ +
Exempt Sources	+
Exempt Destinations/Services	+
Redirect after Captive Portal	[✓ Original Request] Specific URL
Broadcast SSID	●
Schedule	always
Block Intra-SSID Traffic	●
Broadcast Suppression	● ARPs for known clients ✖ DHCP Uplink ✖ +
Filter clients by MAC Address	
RADIUS server	○
VLAN Pooling	○
Quarantine Host	●

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-exemptoption 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.

Correct Answer: C

QUESTION 2

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

A. PEAP

B. EAP-TTLS

C. EAP-TLS

D. EAP-GTC

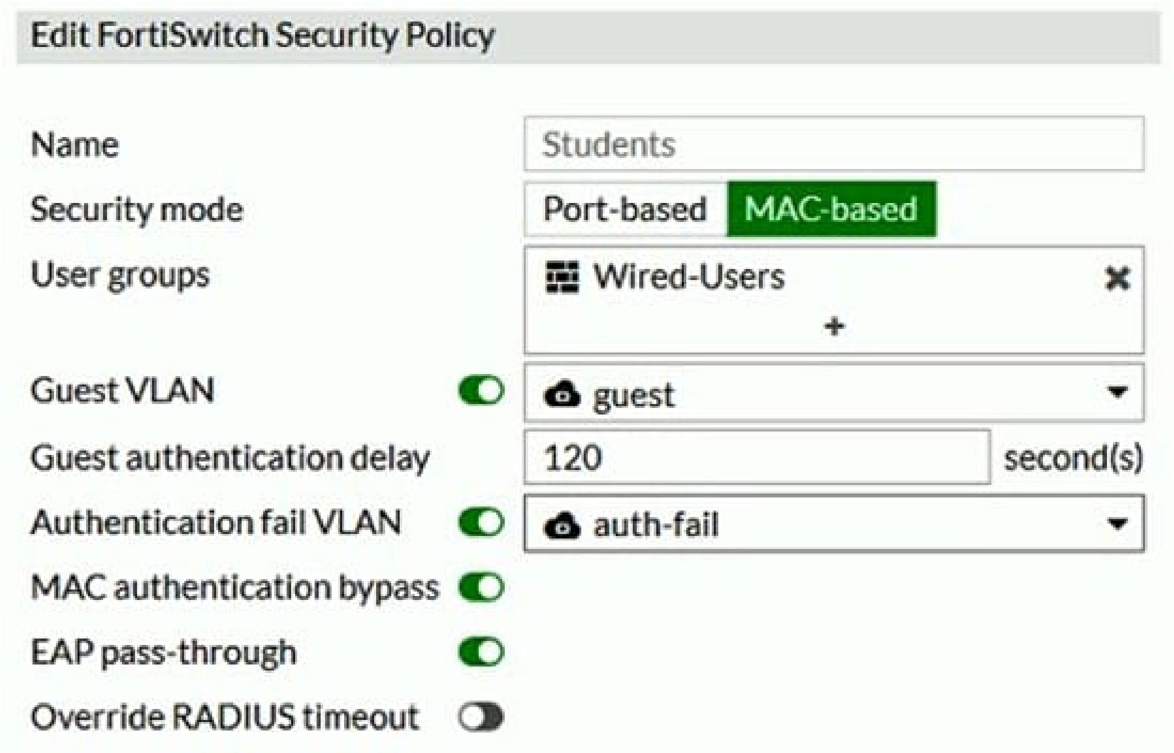
Correct Answer: AC

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

QUESTION 3

Refer to the exhibit.

Examine the configuration of the FortiSwitch security policy profile.



Edit FortiSwitch Security Policy

Name: Students

Security mode: Port-based | **MAC-based**

User groups: Wired-Users ✖ +

Guest VLAN ● guest

Guest authentication delay: 120 second(s)

Authentication fail VLAN ● auth-fail

MAC authentication bypass ●

EAP pass-through ●

Override RADIUS timeout ○

If the security profile shown in the exhibit is assigned on the FortiSwitch port for 802.1X.port authentication, which statement is correct?

A. Host machines that do support 802.1X authentication, but have failed authentication, will be assigned the guest VLAN.

B. All unauthenticated users will be assigned the auth-fail VLAN.

C. Authenticated users that are part of the wired-users group will be assigned the guest VLAN.

D. Host machines that do not support 802.1X authentication will be assigned the guest VLAN.

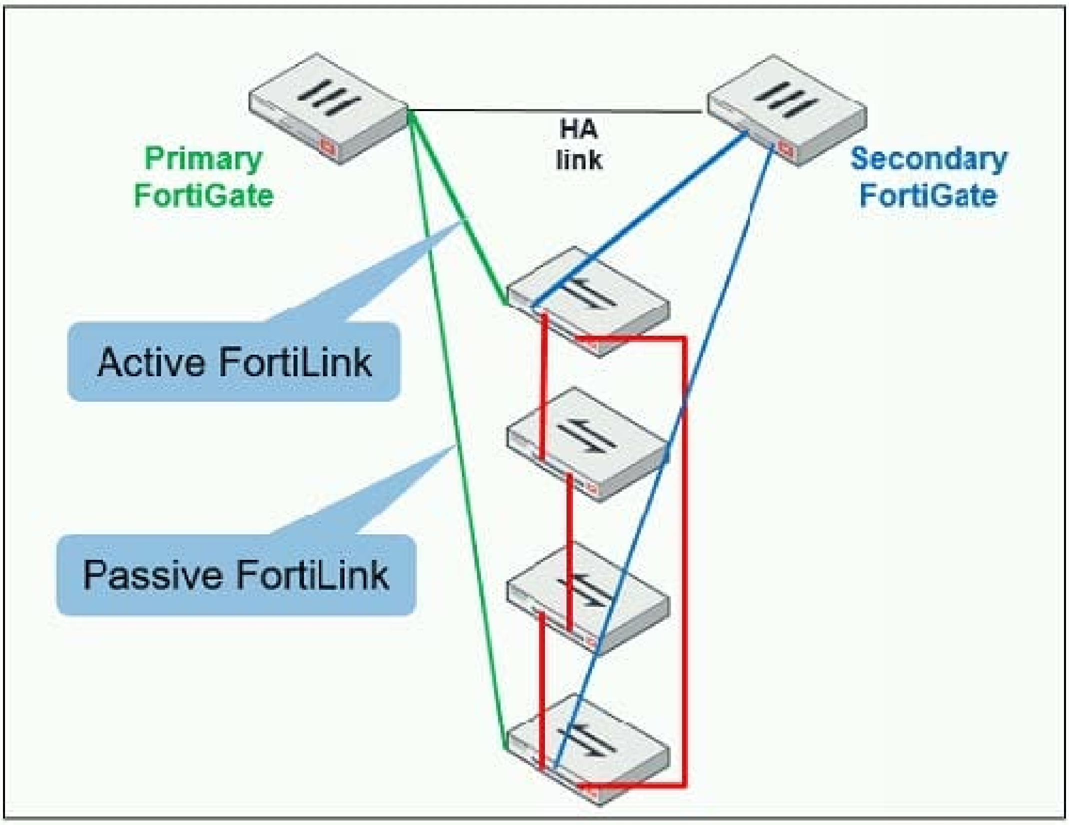
Correct Answer: C

QUESTION 4

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.

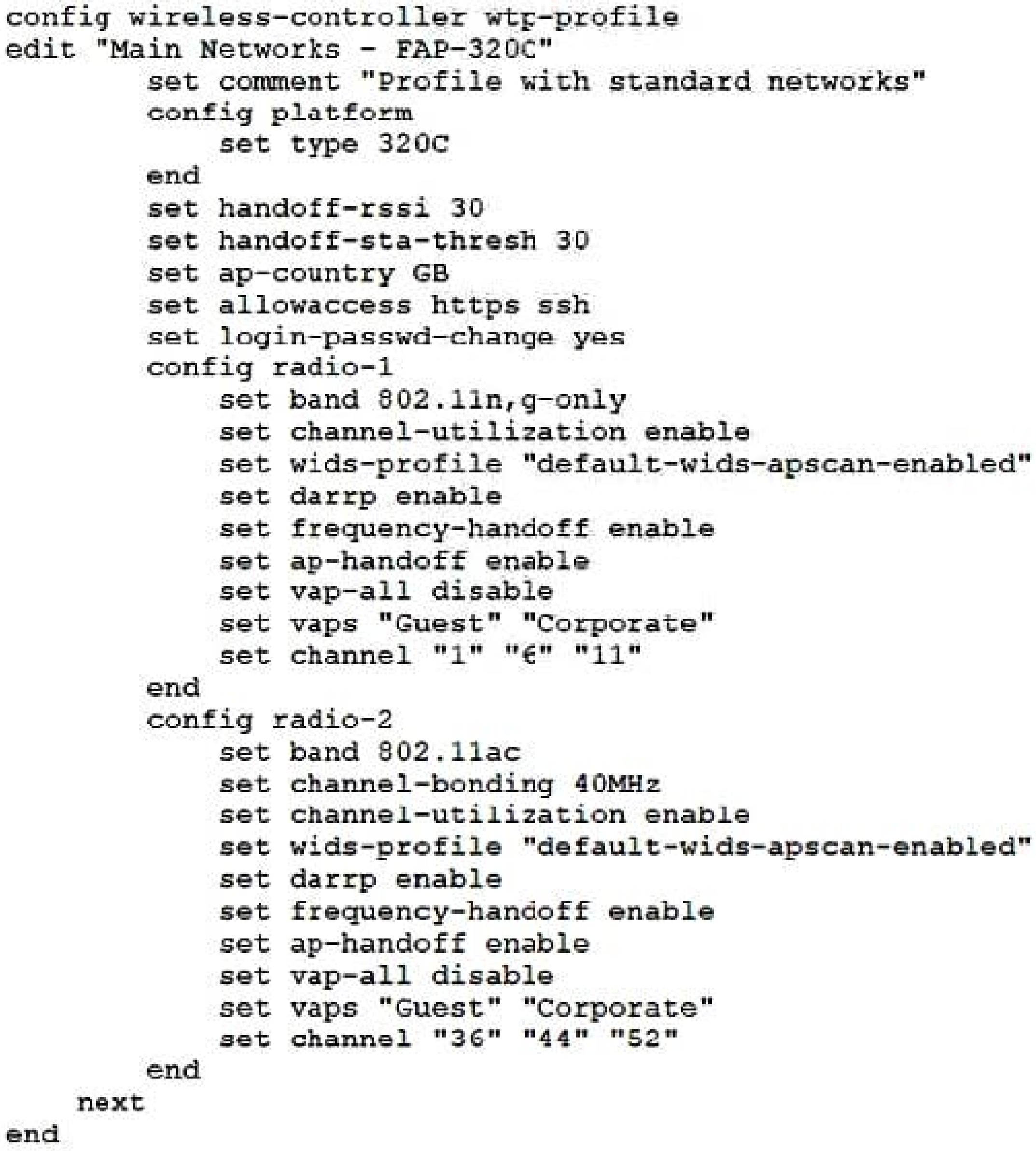
D. Enable STP on the FortiGate interfaces.

Correct Answer: CD

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

QUESTION 5

Refer to the exhibit.



```
config wireless-controller wtp-profile
edit "Main Networks - FAP-320C"
        set comment "Profile with standard networks"
        config platform
            set type 320C
        end
        set handoff-rssi 30
        set handoff-sta-thresh 30
        set ap-country GB
        set allowaccess https ssh
        set login-passwd-change yes
        config radio-1
            set band 802.11n,g-only
            set channel-utilization enable
            set wids-profile "default-wids-apscan-enabled"
            set darrp enable
            set frequency-handoff enable
            set ap-handoff enable
            set vap-all disable
            set vaps "Guest" "Corporate"
            set channel "1" "€" "11"
        end
        config radio-2
            set band 802.11ac
            set channel-bonding 40MHz
            set channel-utilization enable
            set wids-profile "default-wids-apscan-enabled"
            set darrp enable
            set frequency-handoff enable
            set ap-handoff enable
            set vap-all disable
            set vaps "Guest" "Corporate"
            set channel "36" "44" "52"
        end
    next
end
```

In the WTP profile configuration shown in the exhibit, the AP profile is assigned to two FAP-320 APs that are installed in an open plan office.

1.

The first AP has 32 clients associated to the 5GHz radios and 22 clients associated to the 2.4GHz

radio.

2.

The second AP has 12 clients associated to the 5GHz radios and 20 clients associated to the 2.4GHz radio.

A dual band-capable client enters the office near the first AP and the first AP measures the new client at ?33 dBm signal strength. The second AP measures the new client at ?43 dBm signal strength.

In the new client attempts to connect to the corporate wireless network, to which AP radio will the client be associated?

A. The second AP 5GHz interface.

B. The first AP 2.4GHz interface.

C. The first AP 5GHz interface.

D. The second AP 2.4GHz interface.

Correct Answer: A