



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.passapply.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

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers





QUESTION 1

Refer to the exhibits.

SSID	Guest
Security Mode	Captive Portal
Client Limit	<input type="checkbox"/>
Portal Type	Authentication Disclaimer + Authentication Disclaimer Only
Authentication Portal	Local External
	https://fac.trainingad.training.lab/guest:
User Groups	<div>guest.portal</div> <div>+</div>
Exempt Sources	<div>+</div>
Exempt Destinations/Services	<div>+</div>
Redirect after Captive Portal	Original Request Specific URL
Broadcast SSID	<input checked="" type="checkbox"/>
Schedule ⓘ	always
Block Intra-SSID Traffic	<input checked="" type="checkbox"/>
Broadcast Suppression	<div><div><input checked="" type="checkbox"/> ARPs for known clients</div><div><input checked="" type="checkbox"/> DHCP Uplink</div><div>+</div></div>
Filter clients by MAC Address	
RADIUS server	<input type="checkbox"/>
VLAN Pooling	<input type="checkbox"/>
Quarantine Host	<input checked="" type="checkbox"/>

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-exemption 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

Refer to the exhibit.

Examine the output of the debug command and port configuration shown in the exhibit.



Debug command output

```
# diagnose switch-controller switch-info mac-table
FS108D3W17002387      0 :
    MAC address      Interface      vlan
=====
78:2b:cb:d8:36:68    port1      4094
```

Port configuration

```
config switch-controller managed-switch
  edit FS108D3W17002387
    config ports
      edit port1
        set learning-limit 1
        set discard-mode all-tagged
        set arp-inspection-trust untrusted
      end
    end
```

FortiGate learned the MAC address 78:2b:cb:d8:36:68 dynamically.

What action does FortiSwitch take if there is an untagged frame coming to port1 will different MAC address?

- A. The frame is accepted and assigned to the quarantine VLAN.
- B. The frame is accepted and FortiSwitch will update its mac address table with the new MAC address.
- C. The frame is dropped.
- D. The frame is accepted and assigned to the user VLAN.

Correct Answer: A

QUESTION 3

Refer to the exhibit.

Examine the packet capture shown in the exhibit, which contains a RADIUS access request packet sent by FortiSwitch to a RADIUS server.



```
> Frame 1: 164 bytes on wire (1312 bits), 164 bytes captured (1312 bits)
> Ethernet II, Src: Vmware_96:70:b5 (00:50:56:96:70:b5), Dst: Vmware_96:d8:76 (00:50:56:96:d8:76)
> Internet Protocol Version 4, Src: 10.0.1.254, Dst: 10.0.1.150
> User Datagram Protocol, Src Port: 48704, Dst Port: 1812
✓ RADIUS Protocol
  Code: Access-Request (1)
  Packet identifier: 0x96 (150)
  Length: 122
  Authenticator: 49a700a9981a2eb044bf811f482412a0
  [The response to this request is in frame 2]
  ✓ Attribute Value Pairs
    > AVP: l=18 t=NAS-Identifier(32): S124DP3X16008048
    > AVP: l=19 t=User-Name(1): 00-E0-4C-36-0D-5E
    > AVP: l=34 t=User-Password(2): Encrypted
    > AVP: l=6 t=NAS-Port-Type(61): Ethernet(15)
    > AVP: l=19 t=Calling-Station-Id(31): 00-E0-4C-36-0D-5E
    > AVP: l=6 t=Service-Type(6): Call-Check(10)
```

Why does the User-Name field in the RADIUS access request packet contain a MAC address?

- A. The FortiSwitch interface is configured for 802.1X port authentication with MAC address bypass, and the connected device does not support 802.1X.
- B. FortiSwitch authenticates itself using its MAC address as the user name.
- C. The connected device is doing machine authentication.
- D. FortiSwitch is replying to an access challenge packet sent by the RADIUS server and requesting the client MAC address.

Correct Answer: D

QUESTION 4

A wireless network in a school provides guest access using a captive portal to allow unregistered users to self-register and access the network. The administrator is requested to update the existing configuration to provide captive portal authentication through a secure connection (HTTPS) to protect and encrypt guest user credentials after they receive the login information when registered for the first time.

Which two changes must the administrator make to enforce HTTPS authentication? (Choose two.)

- A. Provide instructions to users to use HTTPS to access the network.
- B. Create a new SSID with the HTTPS captive portal URL.
- C. Enable Redirect HTTP Challenge to a Secure Channel (HTTPS) in the user authentication settings
- D. Update the captive portal URL to use HTTPS on FortiGate and FortiAuthenticator

Correct Answer: BD

**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" "6" "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
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

[Latest NSE7_SAC-6.2 Dumps](#)

[NSE7_SAC-6.2 PDF Dumps](#)

[NSE7_SAC-6.2 VCE Dumps](#)