

NSE7\_SAC-6.2.VCEplus.premium.exam.30q

Number: NSE7\_SAC-6.2

Passing Score: 800

Time Limit: 120 min

File Version: 1.0



**Website:** <https://vceplus.com>

**VCE to PDF Converter:** <https://vceplus.com/vce-to-pdf/>

**Facebook:** <https://www.facebook.com/VCE.For.All.VN/>

**Twitter :** [https://twitter.com/VCE\\_Plus](https://twitter.com/VCE_Plus)

NSE7\_SAC-6.2

Fortinet NSE 7 - Secure Access 6.2



## Exam A

### QUESTION 1

Which step can be taken to ensure that only FortiAP devices receive IP addresses from a DHCP server on FortiGate?

- A. Change the interface addressing mode to FortiAP devices.
- B. Create a reservation list in the DHCP server settings.
- C. Configure a VCI string value of `FortiAP` in the DHCP server settings.
- D. Use DHCP option 138 to assign IPs to FortiAP devices.

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

### QUESTION 2

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.

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

- 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

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 3** 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

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: [https://help.fortinet.com/fauth/3-3/Content/FortiAuthenticator%203%20Admin%20Guide/500/501\\_EAP.htm](https://help.fortinet.com/fauth/3-3/Content/FortiAuthenticator%203%20Admin%20Guide/500/501_EAP.htm)

**QUESTION 4** Which two statements about the use of digital certificates are true?

(Choose two.)

- A. An intermediate CA can sign server certificates.
- B. An intermediate CA can sign another intermediate CA certificate.
- C. The end entity's certificate can only be created by an intermediate CA.
- D. An intermediate CA can validate the end entity certificate signed by another intermediate CA.

**Correct Answer:** BD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 5** 802.1X port authentication is enabled on only those ports that the FortiSwitch security policy is assigned to.

Which configurable items are available when you configure the security policy on FortiSwitch? (Choose two.)

- A. FSSO groups
- B. Security mode
- C. User groups
- D. Default guest group

**Correct Answer:** BC

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 6**

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**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 7**

An administrator is deploying APs that are connecting over an IPsec network. All APs have been configured to connect to FortiGate manually. FortiGate can discover the APs and authorize them. However, FortiGate is unable to establish CAPWAP tunnels to manage the APs.

Which configuration setting can the administrator perform to resolve the problem?

- A. Decrease the CAPWAP tunnel MTU size for APs to prevent fragmentation.
- B. Enable CAPWAP administrative access on the IPsec interface.
- C. Upgrade the FortiAP firmware image to ensure compatibility with the FortiOS version.
- D. Assign a custom AP profile for the remote APs with the `set mpls-connection` option enabled.



**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 8**

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

**Section:** (none)

**Explanation**

**Explanation/Reference:**

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

#### QUESTION 9

What action does FortiSwitch take when it receives a loop guard data packet (LGDP) that was sent by itself?

- A. The receiving port is shut down.
- B. The sending port is shut down
- C. The receiving port is moved to the STP blocking state.
- D. The sending port is moved to the STP blocking state

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <https://www.scribd.com/document/468940309/Secure-Access-6-0-Study-Guide-Online-pdf>

**QUESTION 10** Default VLANs are created on FortiGate when the FortiLink interface is created.

By default, which VLAN is set as **Allowed VLANs** on all FortiSwitch ports?

- A. Sniffer VLAN
- B. Camera VLAN
- C. Quarantine VLAN
- D. Voice VLAN

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 11

What does DHCP snooping MAC verification do?

- A. Drops DHCP release packets on untrusted ports
- B. Drops DHCP packets with no relay agent information (option 82) on untrusted ports
- C. Drops DHCP offer packets on untrusted ports
- D. Drops DHCP packets on untrusted ports when the client hardware address does not match the source MAC address

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <https://docs.fortinet.com/document/fortiswitch/6.4.2/administration-guide/335964/dhcp-snooping> (note)

**QUESTION 12** Which statement correctly describes the quest portal behavior on FortiAuthenticator?



- A. Sponsored accounts cannot authenticate using guest portals.
- B. FortiAuthenticator uses POST parameters and a RADIUS client configuration to map the request to a guest portal for authentication.
- C. All guest accounts must be activated using SMS or email activation codes.
- D. All self-registered and sponsored accounts are listed on the **local Users** GUI page on FortiAuthenticator.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 13

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



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

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

- A. FortiGate will reject the certificate if the OCS server replies that the certificate is unknown.
- B. FortiGate will use the OCS server 10.0.1.150 even when the OCS URL field in the user certificate contains a different OCS server IP address.
- C. FortiGate will use the OCS server 10.0.1.150 even when there is a different OCS IP address in the `ocs-override-server` option under `config user peer`.
- D. FortiGate will invalidate the certificate if the OCS server is unavailable.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**



#### QUESTION 14

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

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 15

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	guest.portal x
	+
Exempt Sources	+
Exempt Destinations/Services	+
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	<input checked="" type="checkbox"/>
	ARPs for known clients x
	DHCP Uplink x
	+
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-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.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**



#### QUESTION 16

Refer to the exhibit.

Examine the configuration of the FortiSwitch security policy profile.

Edit FortiSwitch Security Policy

Name	<input type="text" value="Students"/>		
Security mode	<div style="display: flex; gap: 5px;"> <span>Port-based</span> <span style="background-color: #008000; color: white; padding: 2px 5px;">MAC-based</span> </div>		
User groups	<div style="border: 1px solid #ccc; padding: 5px; display: flex; align-items: center;"> <div style="display: flex; align-items: center; gap: 10px;"> <span>Wired-Users</span> <span>×</span> </div> <div style="margin-left: 20px;">+</div> </div>		
Guest VLAN	<input checked="" type="checkbox"/>	<div style="border: 1px solid #ccc; padding: 2px; display: flex; align-items: center;"> <span>guest</span> <span>▼</span> </div>	
Guest authentication delay	<input type="text" value="120"/>	second(s)	
Authentication fail VLAN	<input checked="" type="checkbox"/>	<div style="border: 1px solid #ccc; padding: 2px; display: flex; align-items: center;"> <span>auth-fail</span> <span>▼</span> </div>	
MAC authentication bypass	<input checked="" type="checkbox"/>		
EAP pass-through	<input checked="" type="checkbox"/>		
Override RADIUS timeout	<input type="checkbox"/>		

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

**Section:** (none)

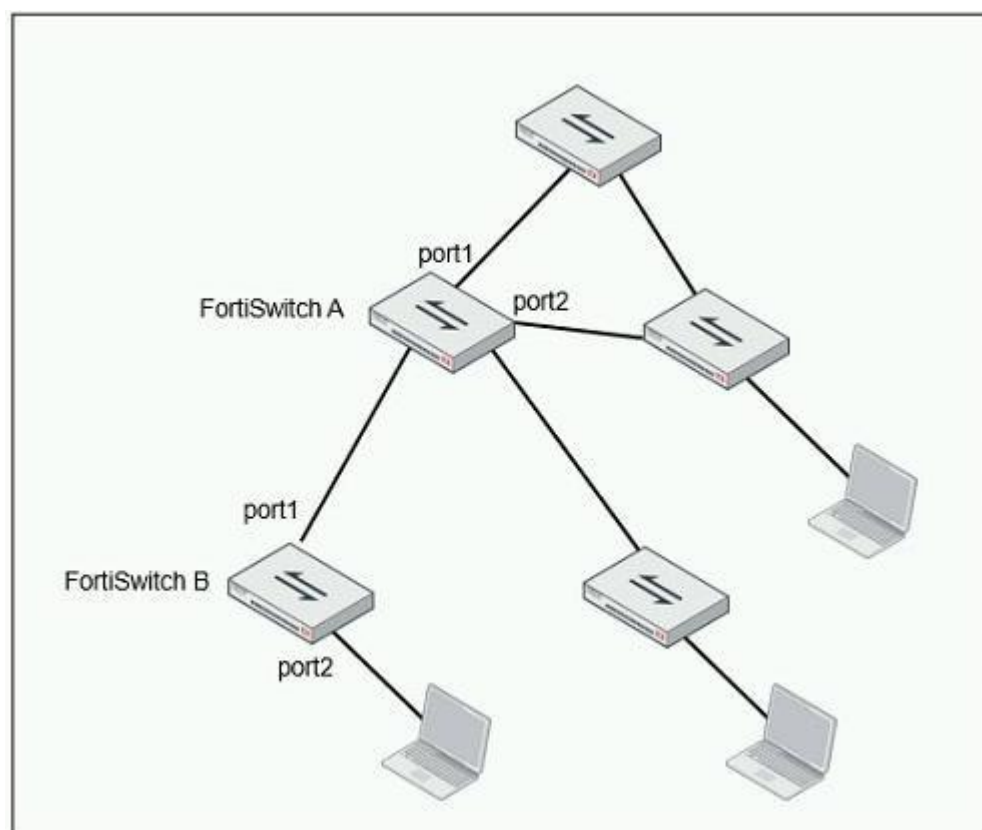
**Explanation**

**Explanation/Reference:**

#### QUESTION 17

Refer to the exhibit.

Examine the network topology shown in the exhibit.



Which port should have root guard enabled?

- A. FortiSwitch A, port2 B.
- FortiSwitch A, port1 C.
- FortiSwitch B, port1
- D. FortiSwitch B, port2



**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <https://docs.fortinet.com/document/fortiswitch/6.4.2/administration-guide/364614/spanning-tree-protocol>

#### QUESTION 18

Examine the following RADIUS configuration:

```

config user radius
  edit "FAC-Lab"
    set server "10.0.1.150"
    set secret ENC XXX
    set nas-ip 10.1.0.254
  next

```

An administrator has configured a RADIUS server on FortiGate that points to FortiAuthenticator. FortiAuthenticator is acting as an authentication proxy and is configured to relay all authentication requests to a remote Windows AD server using LDAP.

While testing the configuration, the administrator notices that the `diagnose test authserver` command works with PAP, however, authentication requests fail when using MSCHAPv2. Which

two changes should the administrator make to get MSCHAPv2 to work? (Choose two.)

- A. Force FortiGate to use the PAP authentication method in the RADIUS server configuration.

- B. Change the remote authentication server from LDAP to RADIUS on FortiAuthenticator.
- C. Use MSCHAP instead of using MSCHAPv2
- D. Enable **Windows Active Directory Domain Authentication** on FortiAuthenticator to add FortiAuthenticator to the Windows domain.

**Correct Answer:** BD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

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

#### QUESTION 19

Refer to the exhibits.

```
config wireless-controller vap
  edit "Corp"
    set vdom "root"
    set ssid "Corp"
    set security wpa2-only-enterprise
    set auth radius
    set radius-server "FAC-Lab"
    set intra-vap-privacy enabled
    set schedule "always"
    set vlan-pooling wtp-group
    config vlan-pool
      edit 101
        set wtp-group "Floor 1"
      next
      edit 102
        set wtp-group "Office"
      next
    end
  next
end
```



Examine the VAP configuration and the WiFi zones table shown in the exhibits.

WiFi (1)					
	Corp (WiFi) SSID: Corp	10.0.3.1 255.255.255.0	WiFi SSID	3	
Zone (3)					
	Corp.zone		Zone	0	
	Corp.101	0.0.0.0 0.0.0.0	VLAN	1	101
	Corp.102	10.0.20.1 255.255.255.0	VLAN	2	102

Which two statements describe FortiGate behavior regarding assignment of VLANs to wireless clients? (Choose two.)

- A. FortiGate will load balance clients using VLAN 101 and VLAN 102 and assign them an IP address from the 10.0.3.0/24 subnet.
- B. Clients connecting to APs in the Floor 1 group will not be able to receive an IP address.
- C. All clients connecting to the Corp SSID will receive an IP address from the 10.0.3.1/24 subnet.
- D. Clients connecting to APs in the Office group will be assigned an IP address from the 10.0.20.1/24 subnet.

**Correct Answer:** BD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 20** 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

**Section:** (none)

**Explanation**

**Explanation/Reference:**

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

**QUESTION 21**

Refer to the exhibit.

Examine the partial debug output shown in the exhibit.





```

FortiGate # diagnose test authserver ldap Training-Lab student password
[2168] handle_req-Rcvd auth req 1584903618 for student in Training-Lab opt=0000001b prot=0
[358] __compose_group_list_from_req-Group 'Training-Lab'
[608] fnbamd_pop3_start-student
[1038] __fnbamd_cfg_get_ldap_list_by_server-Loading LDAP server 'Training-Lab'
[1544] fnbamd_ldap_init-search filter is: sAMAccountName=student
[1553] fnbamd_ldap_init-search base is: cn=users,dc=trainingad,dc=training,dc=lab
[973] __fnbamd_ldap_dns_cb-Resolved Training-Lab(idx 0) to 10.0.1.10
[1021] __fnbamd_ldap_dns_cb-Still connecting.
[517] create_auth_session-Total 1 server(s) to try
[939] __ldap_connect-tcps_connect(10.0.1.10) is established.
[814] __ldap_rxtx-state 3(Admin Binding)
[196] __ldap_build_bind_req-Binding to 'CN=Administrator,CN=Users,DC=trainingAD,DC=training,DC=lab'
[852] fnbamd_ldap_send-sending 80 bytes to 10.0.1.10
[864] fnbamd_ldap_send-Request is sent. ID 1
[814] __ldap_rxtx-state 4(Admin Bind resp)
[1056] fnbamd_ldap_recv-Response len: 16, svr: 10.0.1.10
[756] fnbamd_ldap_parse_response-Got one MESSAGE. ID:1, type:bind
[791] fnbamd_ldap_parse_response-ret=0
[881] __ldap_rxtx-Change state to 'DN search'
[814] __ldap_rxtx-state 11(DN search)
[584] fnbamd_ldap_build_dn_search_req-base:'cn=users,dc=trainingad,dc=training,dc=lab' filter:sAMAccountName=student
[852] fnbamd_ldap_send-sending 99 bytes to 10.0.1.10
[864] fnbamd_ldap_send-Request is sent. ID 2
[814] __ldap_rxtx-state 12(DN search resp)
[1056] fnbamd_ldap_recv-Response len: 69, svr: 10.0.1.10
[756] fnbamd_ldap_parse_response-Got one MESSAGE. ID:2, type:search-entry
[791] fnbamd_ldap_parse_response-ret=0
[1095] __fnbamd_ldap_dn_entry-Get DN 'CN=student,CN=Users,DC=trainingAD,DC=training,DC=lab'
[90] ldap_dn_list_add-added CN=student,CN=Users,DC=trainingAD,DC=training,DC=lab
[1056] fnbamd_ldap_recv-Response len: 16, svr: 10.0.1.10
[756] fnbamd_ldap_parse_response-Got one MESSAGE. ID:2, type:search-result
[791] fnbamd_ldap_parse_response-ret=0
[881] __ldap_rxtx-Change state to 'User Binding'
[814] __ldap_rxtx-state 5(User Binding)
[429] fnbamd_ldap_build_userbind_req-Trying DN 'CN=student,CN=Users,DC=trainingAD,DC=training,DC=lab'
[196] __ldap_build_bind_req-Binding to 'CN=student,CN=Users,DC=trainingAD,DC=training,DC=lab'
[852] fnbamd_ldap_send-sending 105 bytes to 10.0.1.10
[864] fnbamd_ldap_send-Request is sent. ID 3
[814] __ldap_rxtx-state 6(User Bind resp)
[1056] fnbamd_ldap_recv-Response len: 16, svr: 10.0.1.10
[756] fnbamd_ldap_parse_response-Got one MESSAGE. ID:3, type:bind
[791] fnbamd_ldap_parse_response-ret=0
[881] __ldap_rxtx-Change state to 'Attr query'
[814] __ldap_rxtx-state 7(Attr query)
[482] fnbamd_ldap_build_attr_search_req-Adding attr 'memberOf'
[194] fnbamd_ldap_build_attr_search_req-base:'CN=student,CN=Users,DC=trainingAD,DC=training,DC=lab' filter:cn=*
[852] fnbamd_ldap_send-sending 128 bytes to 10.0.1.10
[864] fnbamd_ldap_send-Request is sent. ID 4

```

Which two statements about the debug output are true? (Choose two.)



- A. The connection to the LDAP server timed out.
- B. The user authenticated successfully.
- C. The LDAP server is configured to use regular bind.
- D. The debug output shows multiple user authentications.

**Correct Answer:** BC

**Section:** (none)

**Explanation**

**Explanation/Reference:**

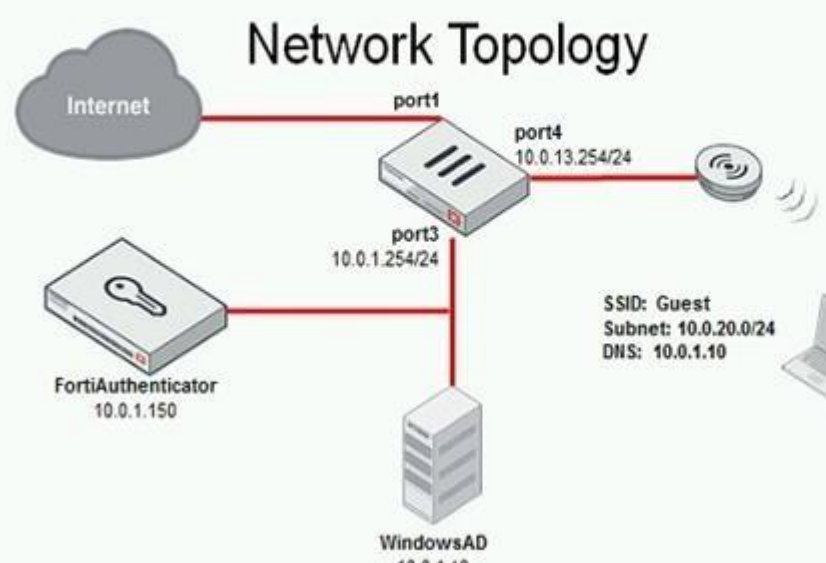
**QUESTION 22**

Refer to the exhibit.

The exhibit shows a network topology and SSID settings.



### Network Topology



SSID: Guest

Security Mode: Captive Portal

Client Limit: ☐

Portal Type: Authentication

Authentication Portal: Local External

User Groups: guest.portal

Exempt Sources: +

Exempt Destinations/Services: FortiAuthenticator, WindowsAD

Redirect after Captive Portal: Original Request

Broadcast SSID: ☒

Schedule: always

Block Intra-SSID Traffic: ☒

Broadcast Suppression: ☒

https://fac.trainingad.training.lab/guest

+

+

+

Original Request

Specific URL

always

+

ARPs for known clients

DHCP Uplink

+

ID	Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
<div style="display: flex; align-items: center;"> <div style="margin-right: 10px;"> <div style="border: 1px solid #ccc; padding: 2px;"> <div style="display: flex; align-items: center;"> <div style="margin-right: 5px;">+</div> <div>Guest01 (Guest-Access) → port1</div> </div> </div> </div> </div>										
12	guest internet access	all	all	always	ALL	ACCEPT	Enabled	+	UTM	0 B
<div style="display: flex; align-items: center;"> <div style="margin-right: 10px;"> <div style="border: 1px solid #ccc; padding: 2px;"> <div style="display: flex; align-items: center;"> <div style="margin-right: 5px;">+</div> <div>port2 → port1</div> </div> </div> </div> </div>										
<div style="display: flex; align-items: center;"> <div style="margin-right: 10px;"> <div style="border: 1px solid #ccc; padding: 2px;"> <div style="display: flex; align-items: center;"> <div style="margin-right: 5px;">+</div> <div>port2 → port3</div> </div> </div> </div> </div>										
<div style="display: flex; align-items: center;"> <div style="margin-right: 10px;"> <div style="border: 1px solid #ccc; padding: 2px;"> <div style="display: flex; align-items: center;"> <div style="margin-right: 5px;">+</div> <div>port3 → port1</div> </div> </div> </div> </div>										
<div style="display: flex; align-items: center;"> <div style="margin-right: 10px;"> <div style="border: 1px solid #ccc; padding: 2px;"> <div style="display: flex; align-items: center;"> <div style="margin-right: 5px;">+</div> <div>port3 → port2</div> </div> </div> </div> </div>										
<div style="display: flex; align-items: center;"> <div style="margin-right: 10px;"> <div style="border: 1px solid #ccc; padding: 2px;"> <div style="display: flex; align-items: center;"> <div style="margin-right: 5px;">+</div> <div>port3 → Students</div> </div> </div> </div> </div>										

FortiGate is configured to use an external captive portal. However, wireless users are not able to see the captive portal login page.

Which configuration change should the administrator make to fix the problem?

- A. Create a firewall policy to allow traffic from the **Guest** SSID to **FortiAuthenticator** and **Windows AD** devices.
- B. Enable the `captive-portal-exempt` option in the firewall policy with the ID 10.
- C. Remove **guest.portal** user group in the firewall policy.
- D. **FortiAuthenticator** and **WindowsAD** address objects should be added as exempt sources.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <https://docs.fortinet.com/document/fortigate/6.0.0/handbook/868644/captive-portals>

**QUESTION 23** Which CLI command should an administrator use to view the certificate validation process in real-time?

- A. `diagnose debug application certd -1`
- B. `diagnose debug application fnbamd -1`
- C. `diagnose debug application authd -1`
- D. `diagnose debug application foauthd -1`

**Correct Answer:** B

**Section:** (none)

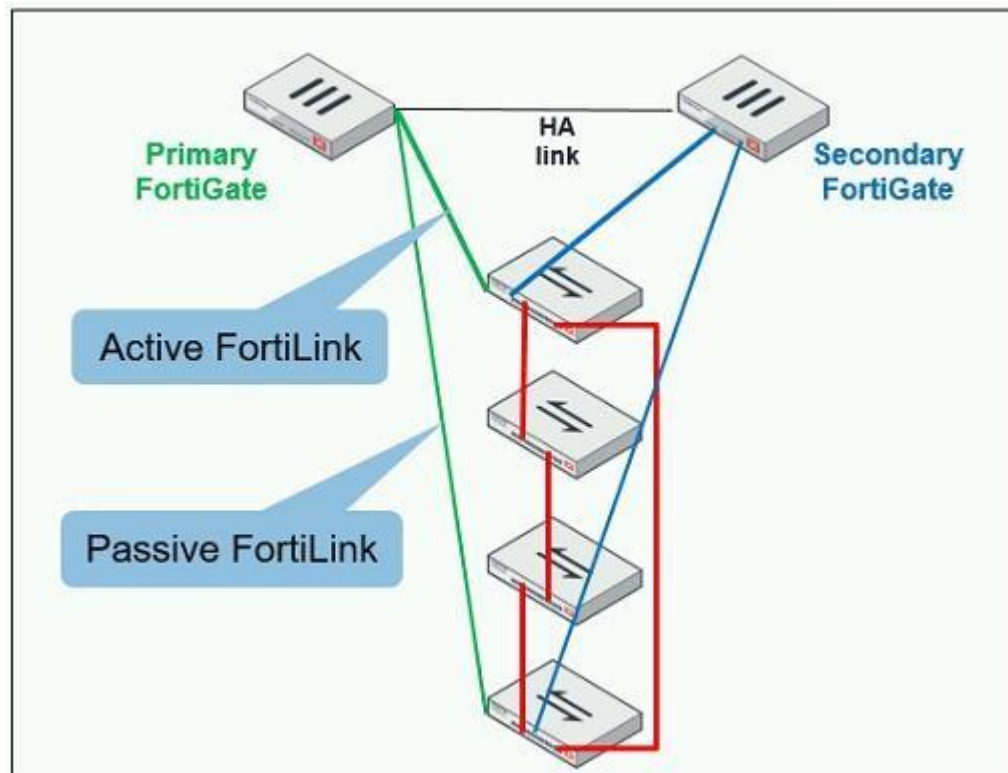
**Explanation**

**Explanation/Reference:**

**QUESTION 24**

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 MLAG-ISL.
- C. Enable `fortilink-split-interface` on the FortiLink interfaces.
- D. Enable STP on the FortiGate interfaces.

Correct Answer: CD

Section: (none)

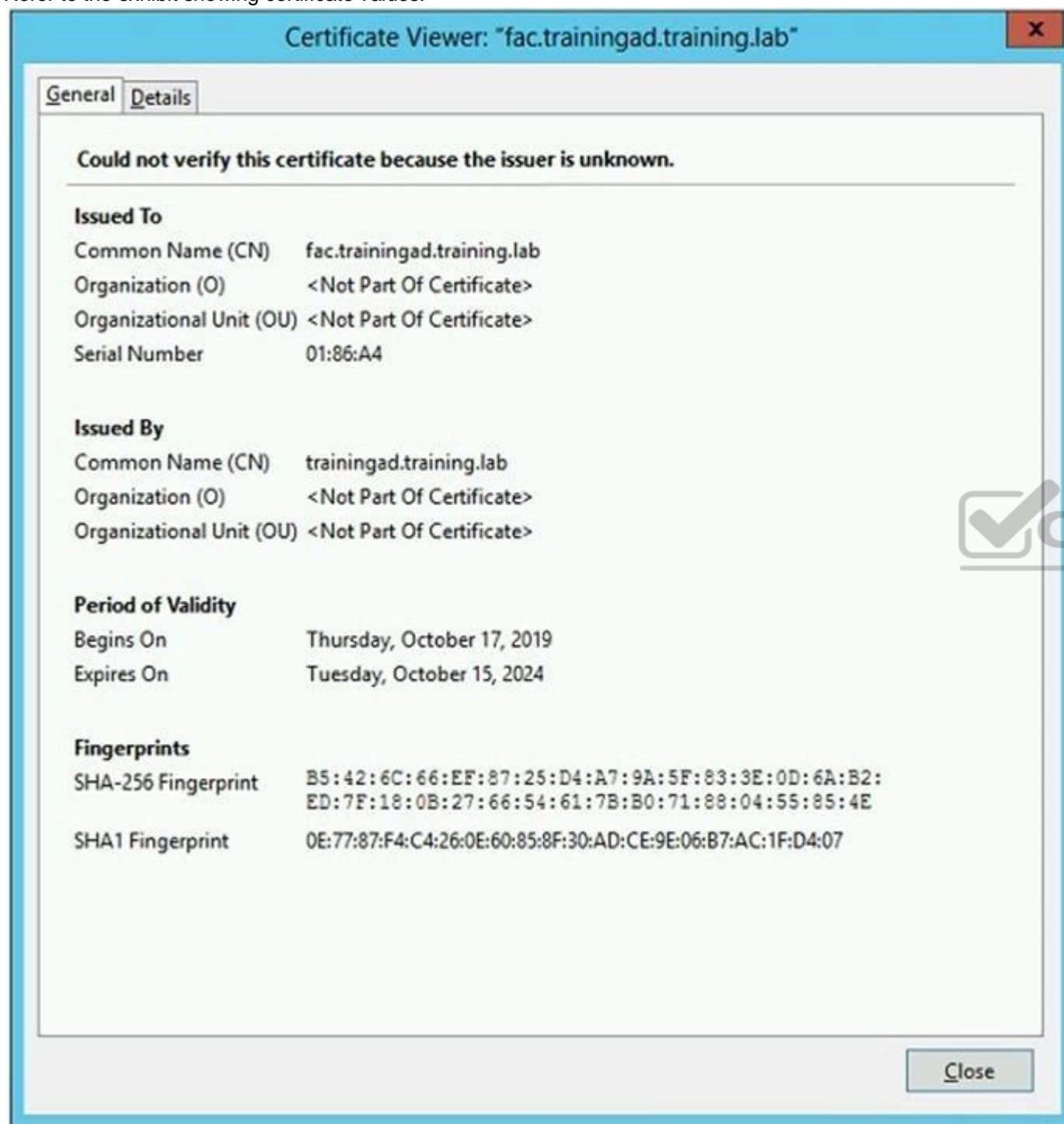
Explanation

Explanation/Reference:

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

#### QUESTION 25

Refer to the exhibit showing certificate values.



Wireless guest users are unable to authenticate because they are getting a certificate error while loading the captive portal login page. This URL string is the HTTPS POST URL guest wireless users see when attempting to access the network using the web browser:

<https://fac.trainingad.training.com/guests/login/?login&post=https://auth.trainingad.training.lab:1003/>

[fgtauth&magic=000a038293d1f411&usermac=b8:27:eb:d8:50:02&apmac=70:4c:a5:9d:0d:28&apip=10.10.100.2&userip=10.0.3.1&ssid=Guest03&apname=PS221ETF18000148&bssid=70:4c:a5:9d:0d:30](https://fac.trainingad.training.com/guests/login/?login&post=https://auth.trainingad.training.lab:1003/fgtauth&magic=000a038293d1f411&usermac=b8:27:eb:d8:50:02&apmac=70:4c:a5:9d:0d:28&apip=10.10.100.2&userip=10.0.3.1&ssid=Guest03&apname=PS221ETF18000148&bssid=70:4c:a5:9d:0d:30)

Which two settings are the likely causes of the issue? (Choose two.)

- A. The external server FQDN is incorrect.
- B. The FortiGate authentication interface address is using HTTPS.
- C. The wireless user's browser is missing a CA certificate.
- D. The user address is not in DDNS form.

**Correct Answer:** AC

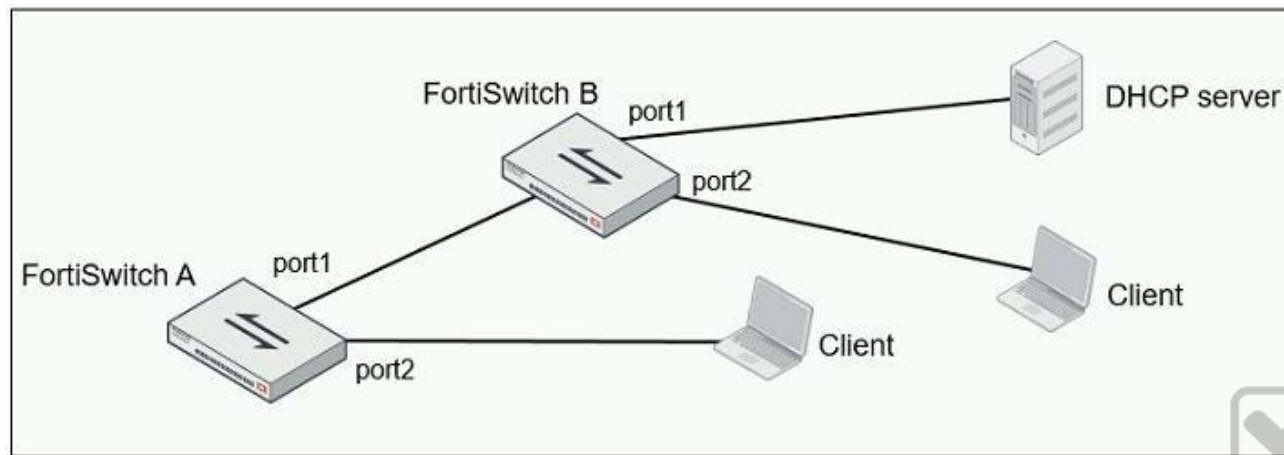
**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 26

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

**Correct Answer:** CD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 27

Examine the following output from the FortiLink real-time debug.

```

FortiGate# diagnose debug application fortilinkd 3
fl_node_apply_switch_port_fgt_properties_update_with_portname[977]:port properties are different for
port(port9) in switch(FS108D3W17002387) old(0x1) new(0x1)o-peer-port() n-peer-port(port2) o-peer-device() n-
peer-device(FGVMEVBB6ITDAO1B)
... flp_event_handler[605]:node: port2 received event 110 state FL_STATE_READY switchname flags 0x26a
... flp_event_handler[605]:node: port2 received event 111 state FL_STATE_READY switchname flags 0x26a
... flp_send_pkt[339]:pkt-sent {type(5) flag=0xe2 node(port2) sw(port2) len(26)smac: 0: c:29:51:dd:a0
dmac:70:4c:a5:24:ba:4f
  
```



Based on the output, what is the status of the communication between FortiGate and FortiSwitch?

- A. FortiGate is unable to authorize the FortiSwitch.
- B. FortiGate is unable to establish FortiLink tunnel to manage the FortiSwitch.
- C. FortiGate is unable to locate a previously managed FortiSwitch.
- D. The FortiLink heartbeat is up.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 28

An administrator has deployed dual band-capable wireless APs in a wireless network. Multiple 2.4 GHz wireless clients are connecting to the network, and subsequent monitoring shows that individual AP 2.4GHz interfaces are being overloaded with wireless connections.

Which configuration change would best resolve the overloading issue?

- A. Configure load balancing AP handoff on both the AP interfaces on all APs.
- B. Configure load balancing AP handoff on only the 2.4GHz interfaces of all APs.
- C. Configure load balancing frequency handoff on both the AP interfaces.
- D. Configure a client limit on the all AP 2.4GHz interfaces.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**



#### QUESTION 29

A FortiGate has the following LDAP configuration.

```
config user ldap
  edit "Training-Lab"
    set server "10.0.1.10"
    set cnid "cn"
    set dn "cn=users,dc=trainingad,dc=training,dc=lab"
    set type regular
    set username "CN=Administrator,DC=trainingAD,DC=training,DC=lab"
    set password ENC XXX
  next
```

On the Windows LDAP server 10.0.1.10, the administrator used `dsquery`, which returned the following output:

```
>dsquery user -samid admin*
"CN=Administrator,CN=Users,DC=trainingAD,DC=training,DC=lab"
```

According to the output, which FortiGate LDAP setting is configured incorrectly?

- A. dn
- B. sAMAccountName
- C. username



D. cnid

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

### QUESTION 30

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

**Section:** (none)

**Explanation**

**Explanation/Reference:**