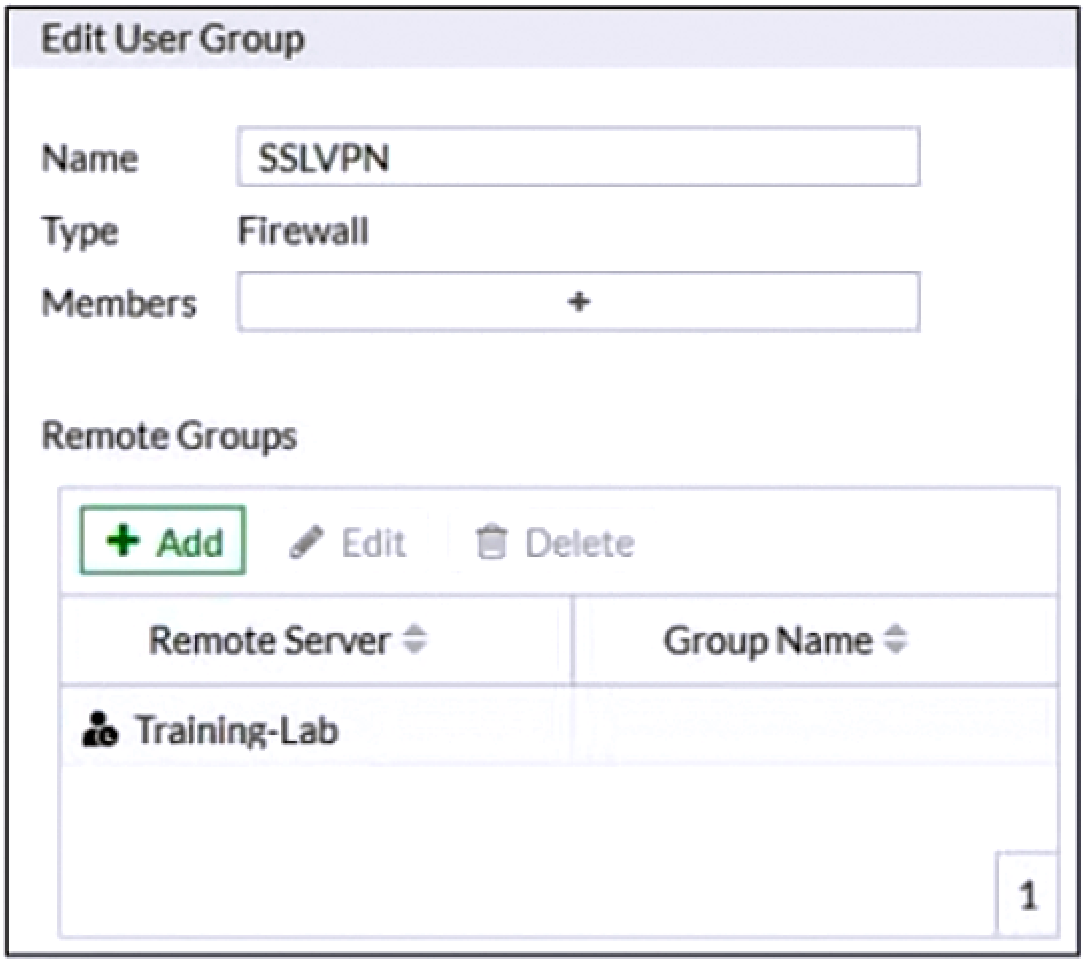
Actual exam question from Fortinet's NSE7_LED-7.0
Question #: 1
Topic #: 1
[All NSE7_LED-7.0 Questions]

Refer to the exhibit.

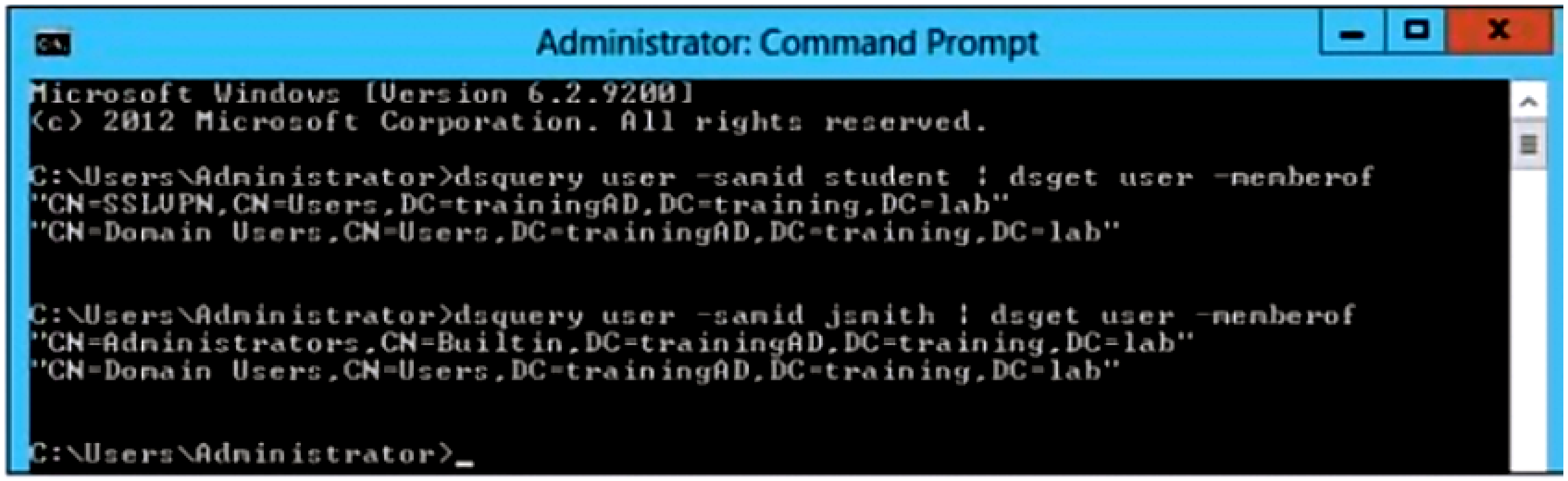


Edit User Group

Name: SSLVPN
Type: Firewall
Members: +

Remote Groups

Remote Server	Group Name
Training-Lab	



```
Microsoft Windows [Version 6.2.9200]
(c) 2012 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>dsquery user -samid student | dsget user -memberof
"CN=SSLVPN,CN=Users,DC=trainingAD,DC=training,DC=lab"
"CN=Domain Users,CN=Users,DC=trainingAD,DC=training,DC=lab"

C:\Users\Administrator>dsquery user -samid jsmith | dsget user -memberof
"CN=Administrators,CN=Builtin,DC=trainingAD,DC=training,DC=lab"
"CN=Domain Users,CN=Users,DC=trainingAD,DC=training,DC=lab"

C:\Users\Administrator>_
```

Examine the FortiGate user group configuration and the Windows AD LDAP group membership information shown in the exhibit.
FortiGate is configured to authenticate SSL VPN users against Windows AD using LDAP. The administrator configured the SSL VPN user group for SSL VPN users.
However, the administrator noticed that both the t and student and jsmith users can connect to SSL VPN.
Which change can the administrator make on FortiGate to restrict the SSL VPN service to the student user only?

A. In the SSL VPN user group configuration, set Group Name to CN=SSLVPN,CN=Users,DC=trainingAD,DC=training,DC=lab.

B. In the SSL VPN user group configuration, change Name to CN=SSLVPN,CN=Users,DC=trainingAD,DC=training,DC=lab.

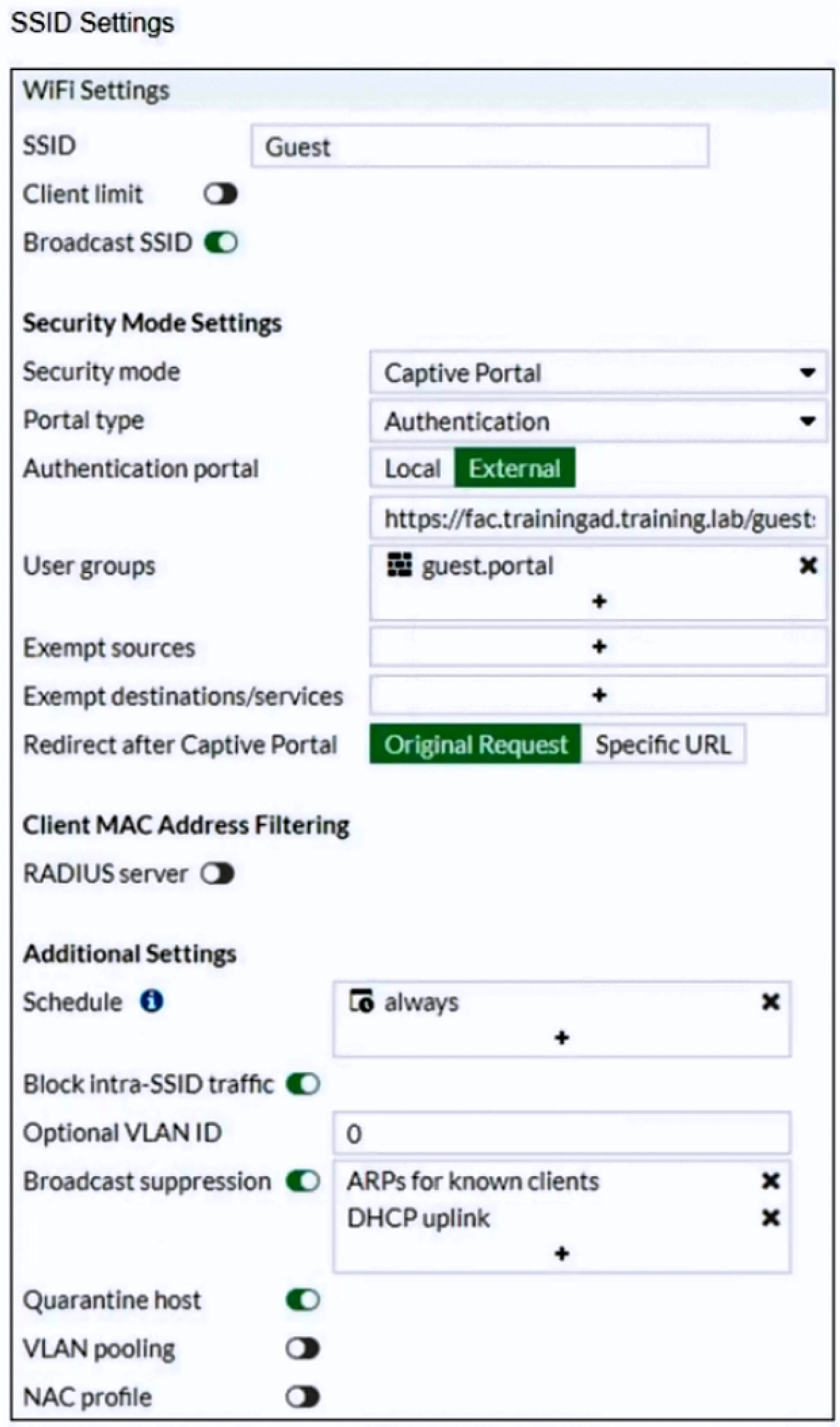
C. In the SSL VPN user group configuration, set Group Name to CN=Domain Users,CN=Users,DC=trainingAD,DC=training,DC=lab.

D. In the SSL VPN user group configuration, change Type to Fortinet Single Sign-On (FSSO).

Show Suggested Answer

Actual exam question from Fortinet's NSE7_LED-7.0
Question #: 2
Topic #: 1
[All NSE7_LED-7.0 Questions]

Refer to the exhibits.



SSID Settings

WiFi Settings

SSID: Guest
Client limit ○
Broadcast SSID ●

Security Mode Settings

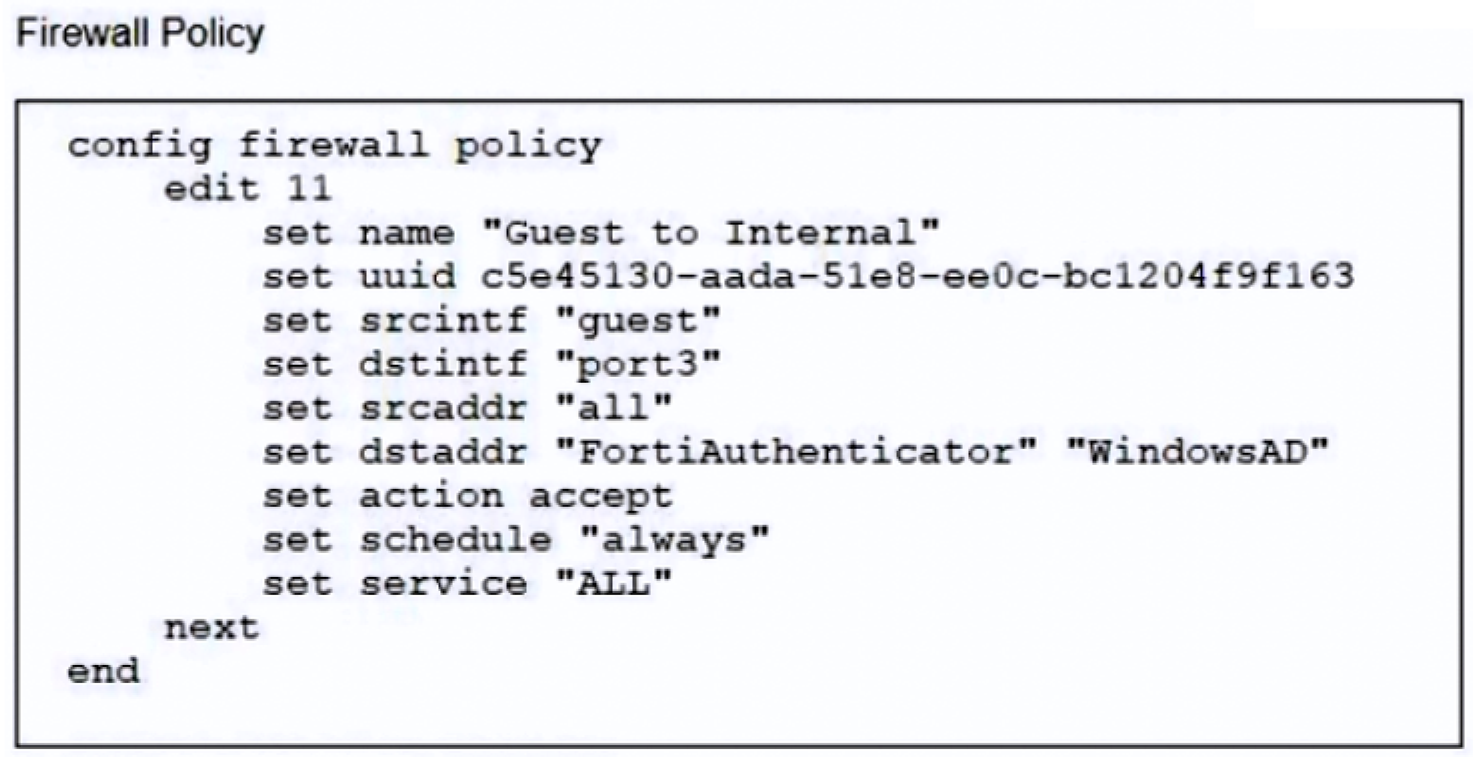
Security mode: Captive Portal
Portal type: Authentication
Authentication portal: Local [✓ External]
https://fac.trainingad.training.lab/guest:
User groups: guest.portal
Exempt sources
Exempt destinations/services
Redirect after Captive Portal: [✓ Original Request] Specific URL

Client MAC Address Filtering

RADIUS server ○

Additional Settings

Schedule: always
Block intra-SSID traffic ●
Optional VLAN ID: 0
Broadcast suppression ●: ARPs for known clients, DHCP uplink
Quarantine host ●
VLAN pooling ○
NAC profile ○



Firewall Policy

```
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
```

Examine the firewall policy configuration and SSID settings.
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. Disable the user group from the SSID configuration.
B. Enable the captive-portal-exempt option in the firewall policy with the ID 11.
C. Apply a guest.portal user group in the firewall policy with the ID 11.
D. Include the wireless client subnet range in the Exempt Source section.

Show Suggested Answer

Actual exam question from Fortinet's NSE7_LED-7.0

Question #: 3

Topic #: 1

[All NSE7_LED-7.0 Questions]

Which two statements about the MAC-based 802.1X security mode available on FortiSwitch are true? (Choose two.)

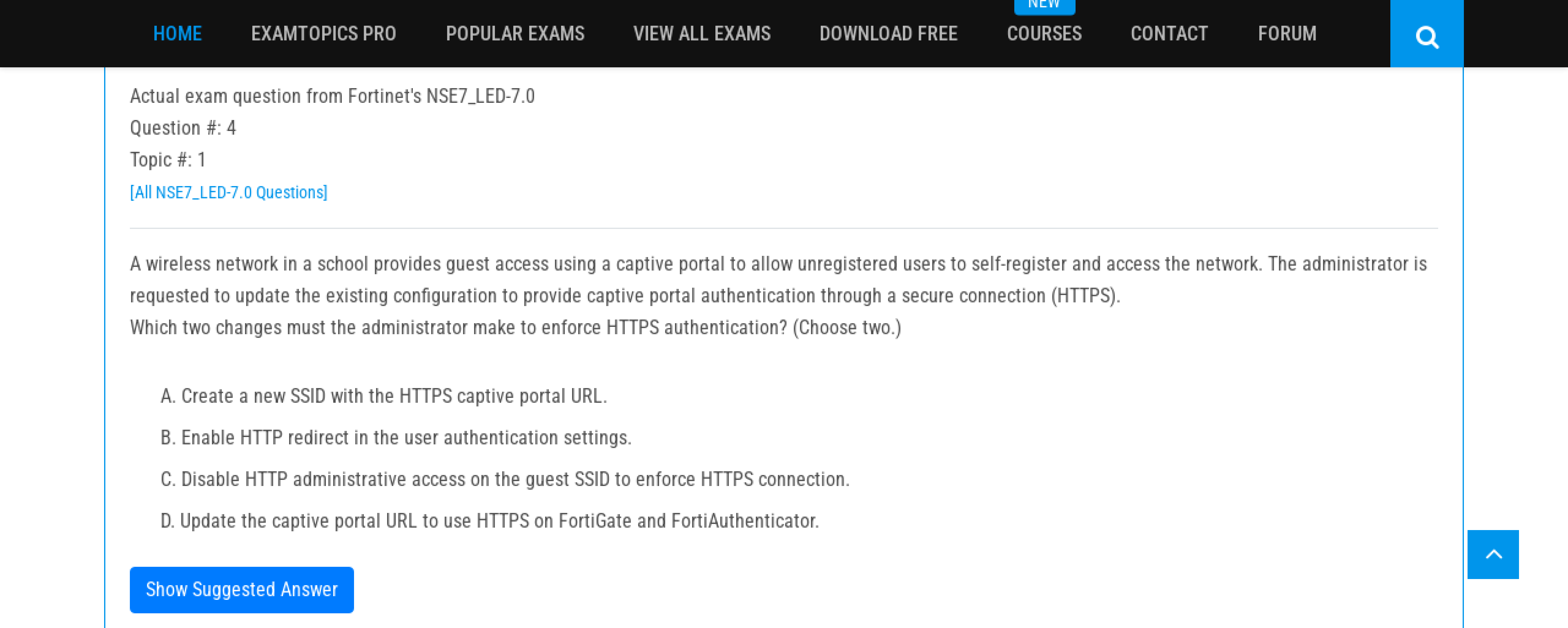
A. FortiSwitch authenticates a single device, and opens the port to other devices connected to the port.

B. FortiSwitch authenticates each device connected to the port.

C. It cannot be used in conjunction with MAC authentication bypass.

D. FortiSwitch can grant different access levels to each device connected to the port.

Show Suggested Answer



Actual exam question from Fortinet's NSE7_LED-7.0
Question #: 4
Topic #: 1
[All NSE7_LED-7.0 Questions]

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

A. Create a new SSID with the HTTPS captive portal URL.

B. Enable HTTP redirect in the user authentication settings.

C. Disable HTTP administrative access on the guest SSID to enforce HTTPS connection.

D. Update the captive portal URL to use HTTPS on FortiGate and FortiAuthenticator.

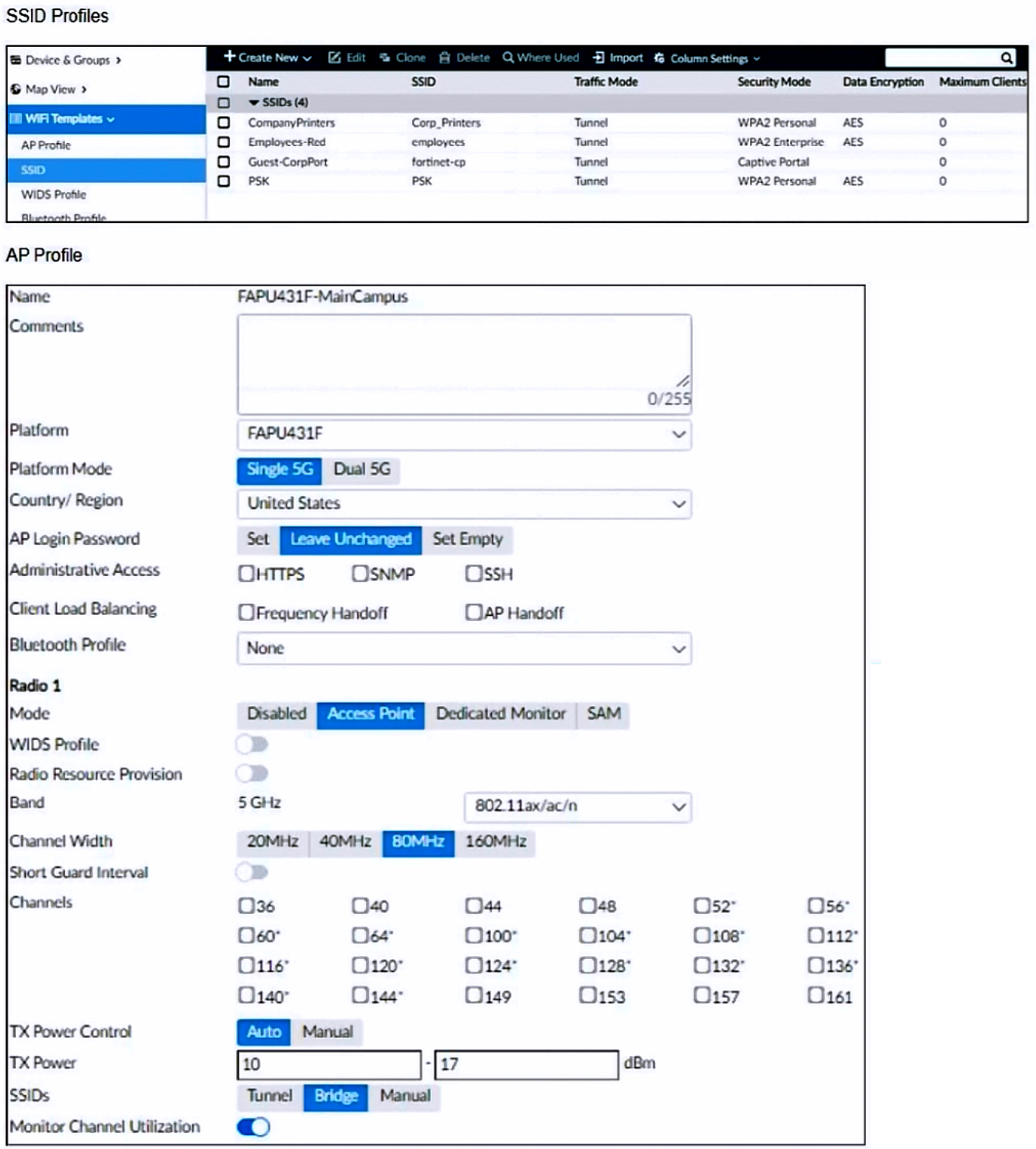
Actual exam question from Fortinet's NSE7_LED-7.0

Question #: 5

Topic #: 1

[All NSE7_LED-7.0 Questions]

Refer to the exhibit.



SSID Profiles

☐	Name	SSID	Traffic Mode	Security Mode	Data Encryption	Maximum Clients
☐	SSIDs (4)					
☐	CompanyPrinters	Corp_Printers	Tunnel	WPA2 Personal	AES	0
☐	Employees-Red	employees	Tunnel	WPA2 Enterprise	AES	0
☐	Guest-CorpPort	fortinet-cp	Tunnel	Captive Portal		0
☐	PSK	PSK	Tunnel	WPA2 Personal	AES	0

AP Profile

Name: FAPU431F-MainCampus

Comments: 0/255

Platform: FAPU431F

Platform Mode: [✓ Single 5G] Dual 5G

Country/ Region: United States

AP Login Password: Set [✓ Leave Unchanged] Set Empty

Administrative Access: □HTTPS □SNMP □SSH

Client Load Balancing: □Frequency Handoff □AP Handoff

Bluetooth Profile: None

Radio 1

Mode: Disabled [✓ Access Point] Dedicated Monitor SAM

WIDS Profile: ○

Radio Resource Provision: ○

Band: 5 GHz 802.11ax/ac/n

Channel Width: 20MHz 40MHz [✓ 80MHz] 160MHz

Short Guard Interval: ○

Channels:

□36 □40 □44 □48 □52* □56*
□60* □64* □100* □104* □108* □112*
□116* □120* □124* □128* □132* □136*
□140* □144* □149 □153 □157 □161

TX Power Control: [✓ Auto] Manual

TX Power: 10 - 17 dBm

SSIDs: Tunnel [✓ Bridge] Manual

Monitor Channel Utilization: ●

The exhibits show the wireless network (VAP) SSID profiles defined on FortiManager and an AP profile assigned to a group of APs that are supported by FortiGate.

None of the APs are broadcasting the SSIDs defined by the AP profile.

Which changes do you need to make to enable the SSIDs to broadcast?

A. In the SSIDs section, enable Tunnel.

B. Enable one channel in the Channels section.

C. Enable multiple channels in the Channels section and enable Radio Resource Provision.

D. In the SSIDs section, enable Manual and assign the networks manually.

Show Suggested Answer

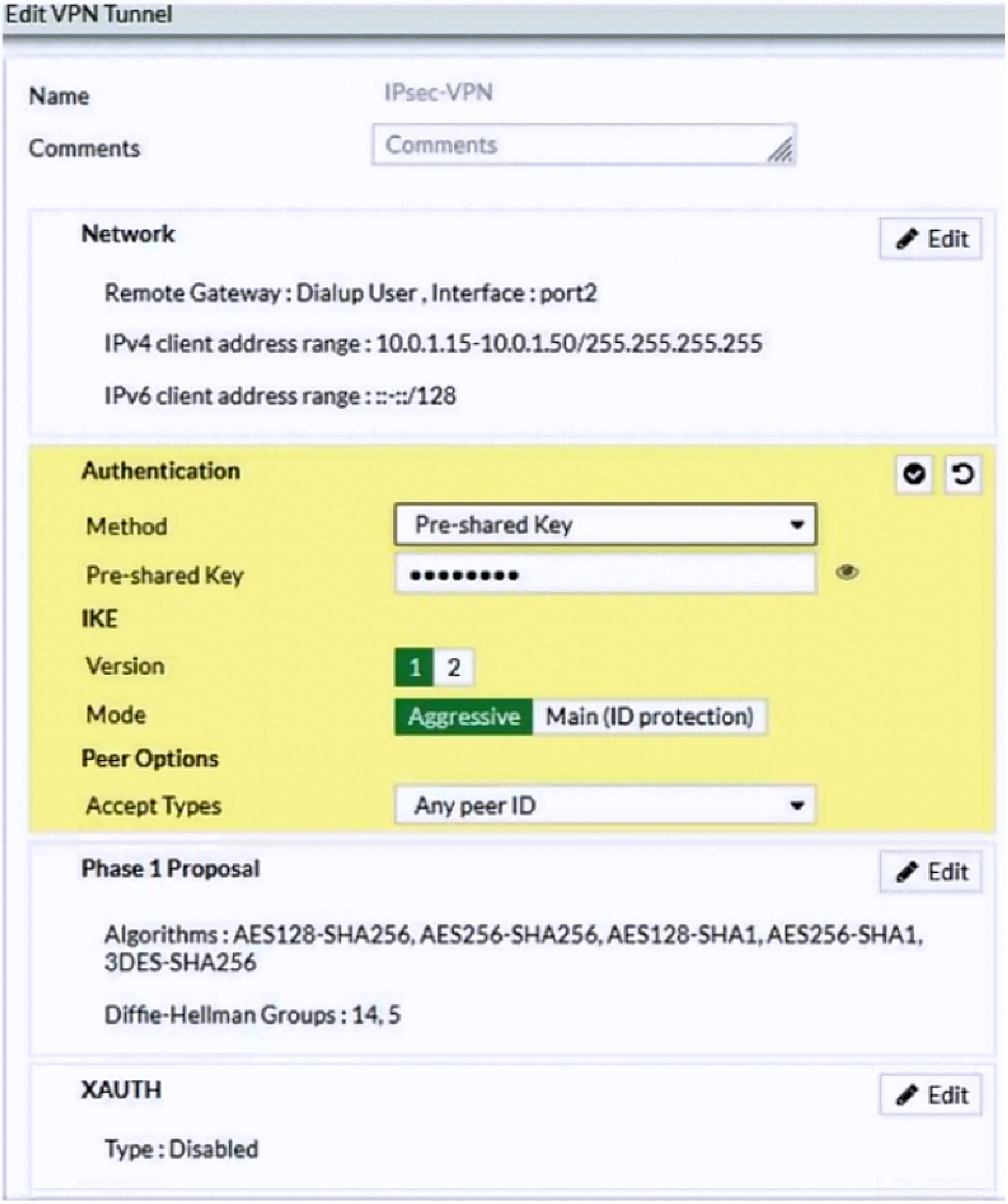
Actual exam question from Fortinet's NSE7_LED-7.0

Question #: 6

Topic #: 1

[All NSE7_LED-7.0 Questions]

Refer to the exhibit.



Edit VPN Tunnel

Name: IPsec-VPN

Comments: Comments

Network

Remote Gateway : Dialup User , Interface : port2

IPv4 client address range : 10.0.1.15-10.0.1.50/255.255.255.255

IPv6 client address range : ::-::/128

Authentication

Method: Pre-shared Key

Pre-shared Key: ●●●●●●●●●

IKE

Version: 1 2

Mode: Aggressive Main (ID protection)

Peer Options

Accept Types: Any peer ID

Phase 1 Proposal

Algorithms : AES128-SHA256, AES256-SHA256, AES128-SHA1, AES256-SHA1, 3DES-SHA256

Diffie-Hellman Groups : 14, 5

XAUTH

Type : Disabled

Examine the IPsec VPN phase 1 configuration shown in the exhibit.

An administrator wants to use certificate-based authentication for an IPsec VPN user.

Which three configuration changes must you make on FortiGate to perform certificate-based authentication for the IPsec VPN user? (Choose three.)

A. Create a PKI user for the IPsec VPN user, and then configure the IPsec VPN tunnel to accept the PKI user as peer certificate.

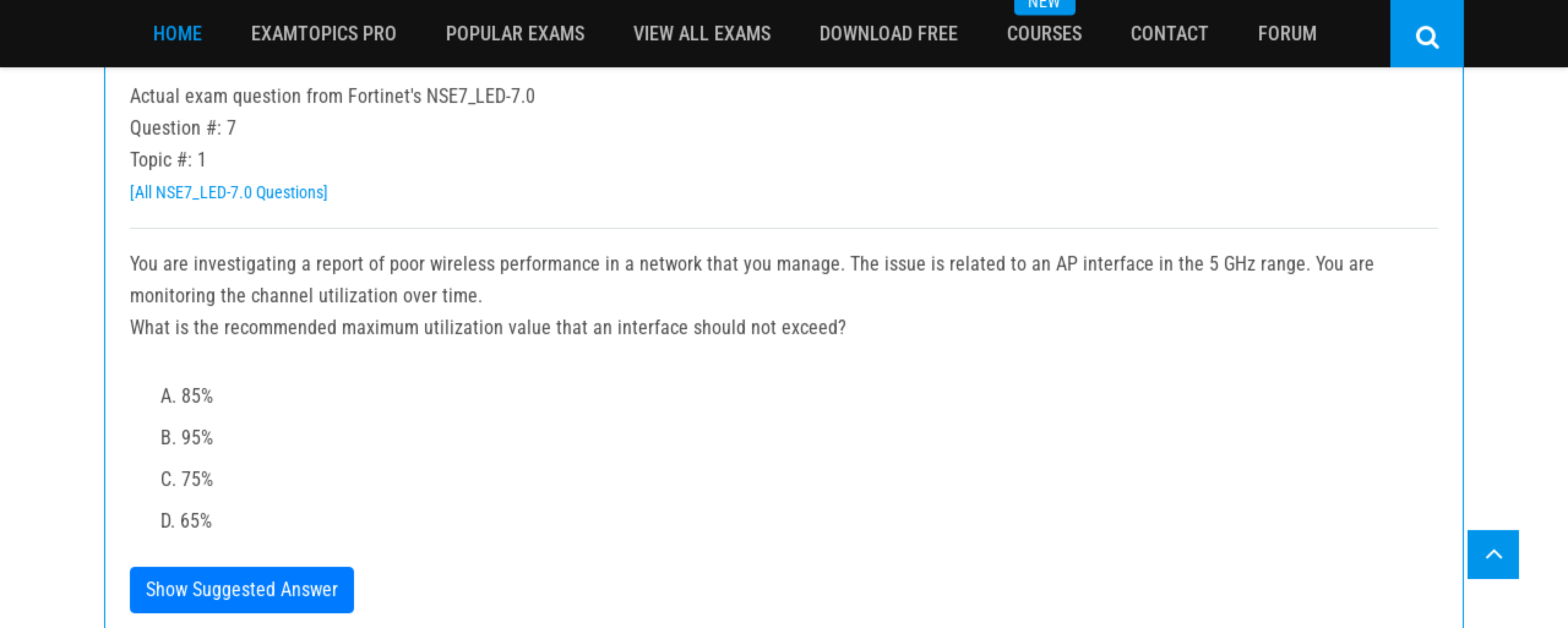
B. In the Authentication section of the IPsec VPN tunnel, in the Method drop-down list, select Signature, and then select the certificate that FortiGate will use for IPsec VPN.

C. In the IKE section of the IPsec VPN tunnel, in the Mode field, select Main (ID protection).

D. Import the CA that signed the user certificate.

E. Enable XAUTH on the IPsec VPN tunnel.

Show Suggested Answer



Actual exam question from Fortinet's NSE7_LED-7.0

Question #: 7

Topic #: 1

[All NSE7_LED-7.0 Questions]

You are investigating a report of poor wireless performance in a network that you manage. The issue is related to an AP interface in the 5 GHz range. You are monitoring the channel utilization over time.

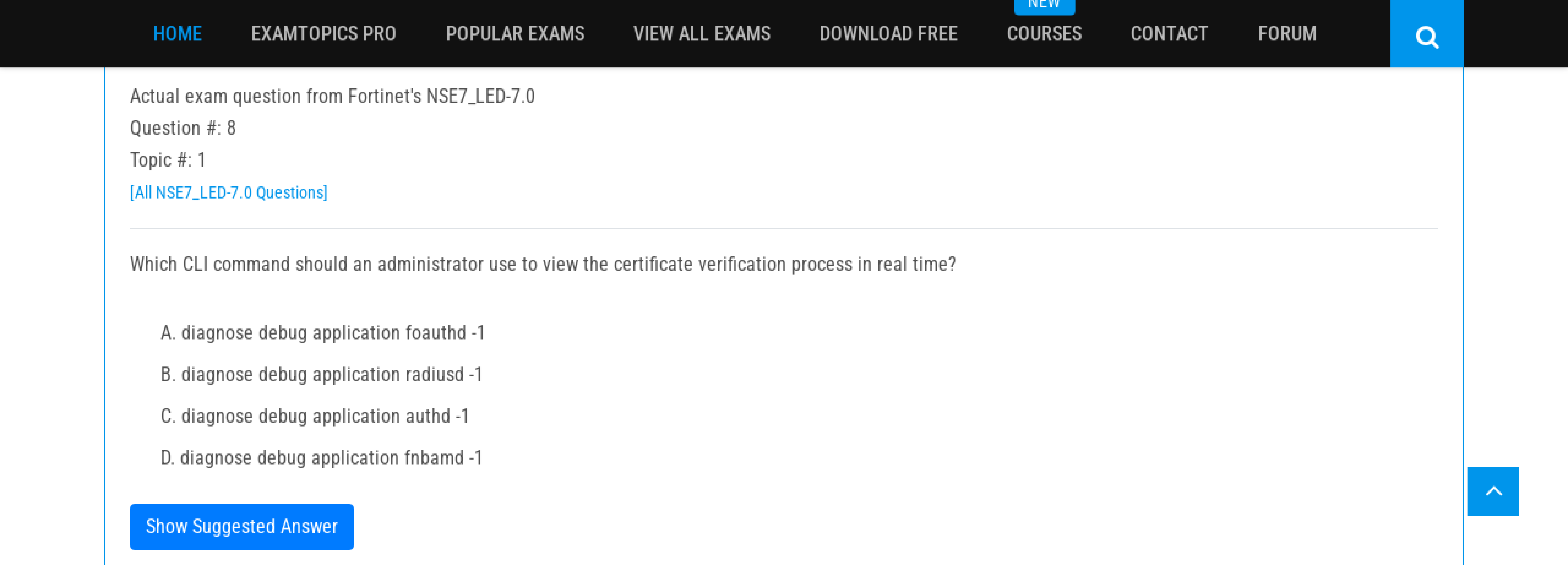
What is the recommended maximum utilization value that an interface should not exceed?

A. 85%

B. 95%

C. 75%

D. 65%



Actual exam question from Fortinet's NSE7_LED-7.0

Question #: 8

Topic #: 1

[All NSE7_LED-7.0 Questions]

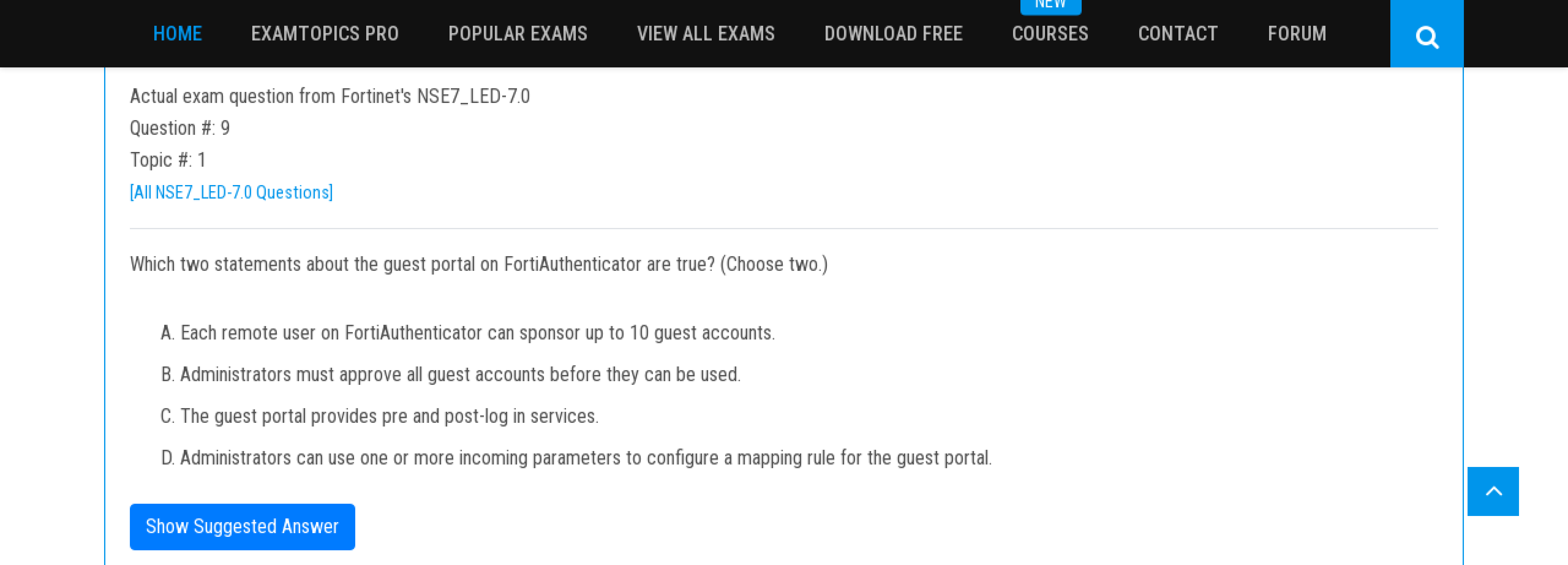
Which CLI command should an administrator use to view the certificate verification process in real time?

A. diagnose debug application foauthd -1

B. diagnose debug application radiusd -1

C. diagnose debug application authd -1

D. diagnose debug application fnbamd -1



Actual exam question from Fortinet's NSE7_LED-7.0

Question #: 9

Topic #: 1

[All NSE7_LED-7.0 Questions]

Which two statements about the guest portal on FortiAuthenticator are true? (Choose two.)

A. Each remote user on FortiAuthenticator can sponsor up to 10 guest accounts.

B. Administrators must approve all guest accounts before they can be used.

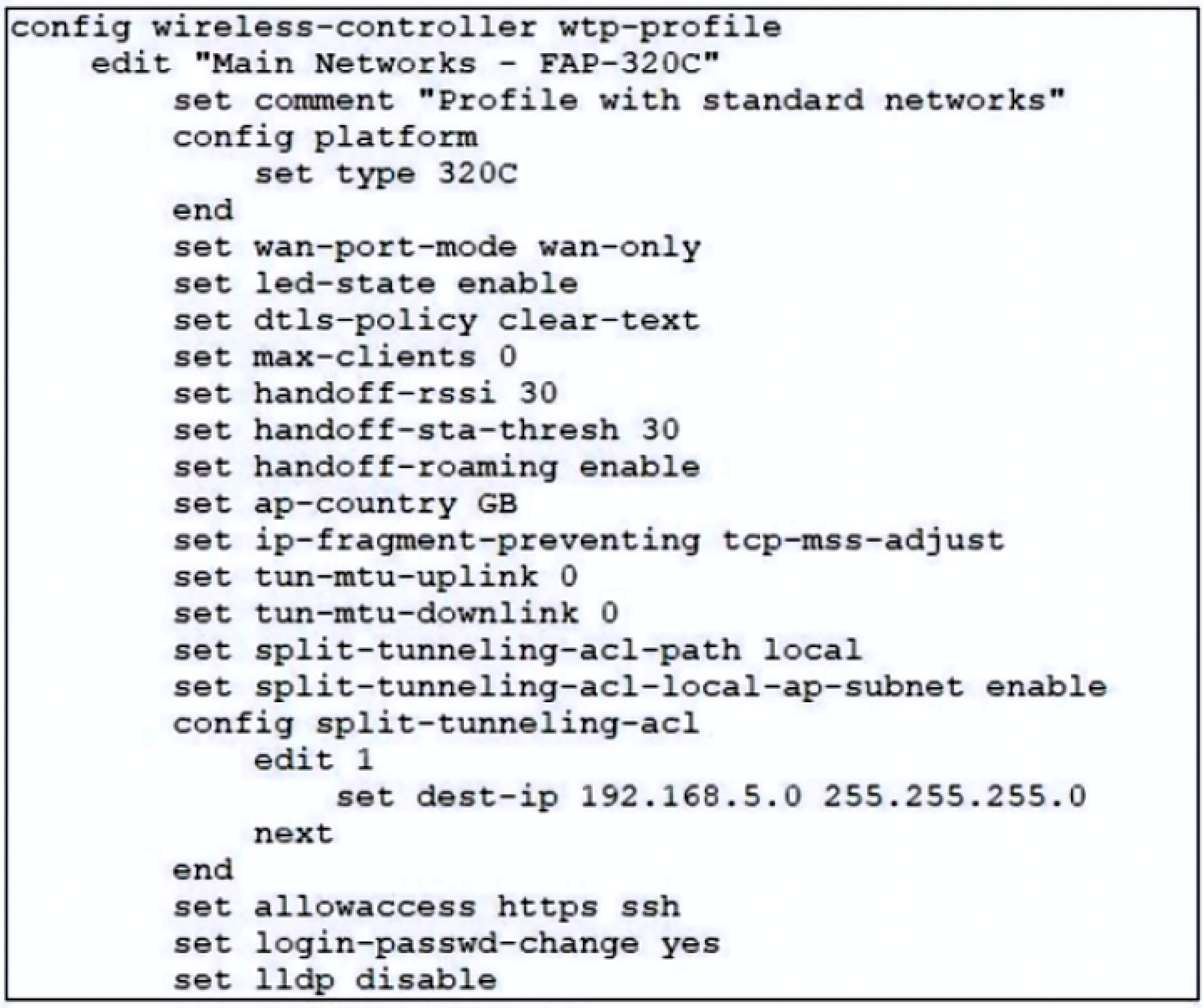
C. The guest portal provides pre and post-log in services.

D. Administrators can use one or more incoming parameters to configure a mapping rule for the guest portal.

Actual exam question from Fortinet's NSE7_LED-7.0
Question #: 10
Topic #: 1
[All NSE7_LED-7.0 Questions]

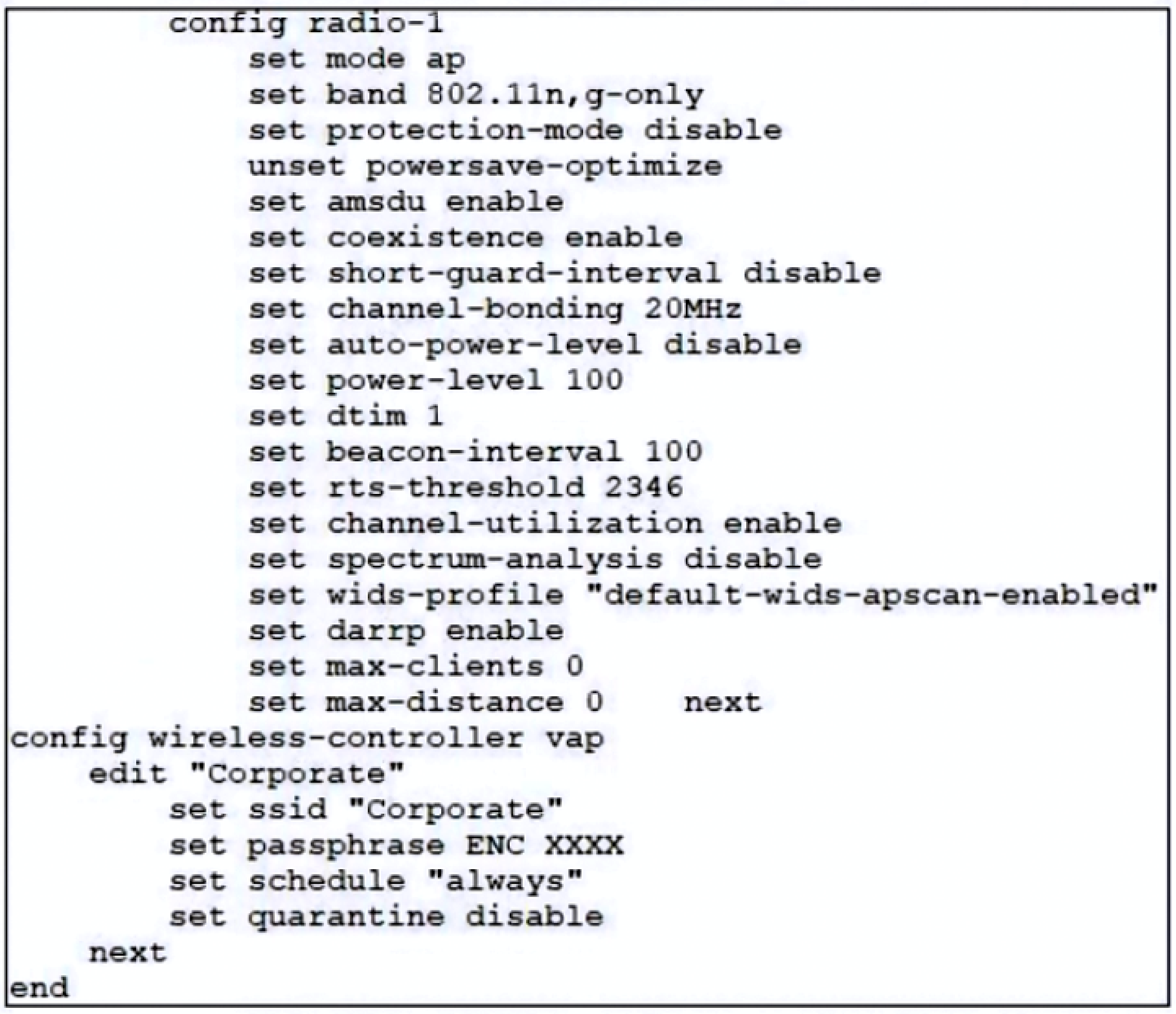
Refer to the exhibits.

Exhibit



```
config wireless-controller wtp-profile
    edit "Main Networks - FAP-320C"
        set comment "Profile with standard networks"
        config platform
            set type 320C
        end
        set wan-port-mode wan-only
        set led-state enable
        set dtls-policy clear-text
        set max-clients 0
        set handoff-rssi 30
        set handoff-sta-thresh 30
        set handoff-roaming enable
        set ap-country GB
        set ip-fragment-preventing tcp-mss-adjust
        set tun-mtu-uplink 0
        set tun-mtu-downlink 0
        set split-tunneling-acl-path local
        set split-tunneling-acl-local-ap-subnet enable
        config split-tunneling-acl
            edit 1
                set dest-ip 192.168.5.0 255.255.255.0
            next
        end
        set allowaccess https ssh
        set login-passwd-change yes
        set lldp disable
```

Exhibit



```
        config radio-1
            set mode ap
            set band 802.11n,g-only
            set protection-mode disable
            unset powersave-optimize
            set amsdu enable
            set coexistence enable
            set short-guard-interval disable
            set channel-bonding 20MHz
            set auto-power-level disable
            set power-level 100
            set dtim 1
            set beacon-interval 100
            set rts-threshold 2346
            set channel-utilization enable
            set spectrum-analysis disable
            set wids-profile "default-wids-apscan-enabled"
            set darrp enable
            set max-clients 0
            set max-distance 0     next
config wireless-controller vap
    edit "Corporate"
        set ssid "Corporate"
        set passphrase ENC XXXX
        set schedule "always"
        set quarantine disable
    next
end
```

In the wireless configuration shown in the exhibits, an AP is deployed in a remote site and has a wireless network (VAP) called Corporate deployed to it.
The network is a tunnelled network; however, clients connecting to a wireless network require access to a local printer. Clients are trying to print to a printer on the remote site, but are unable to do so.
Which configuration change is required to allow clients connected to the Corporate SSID to print locally?

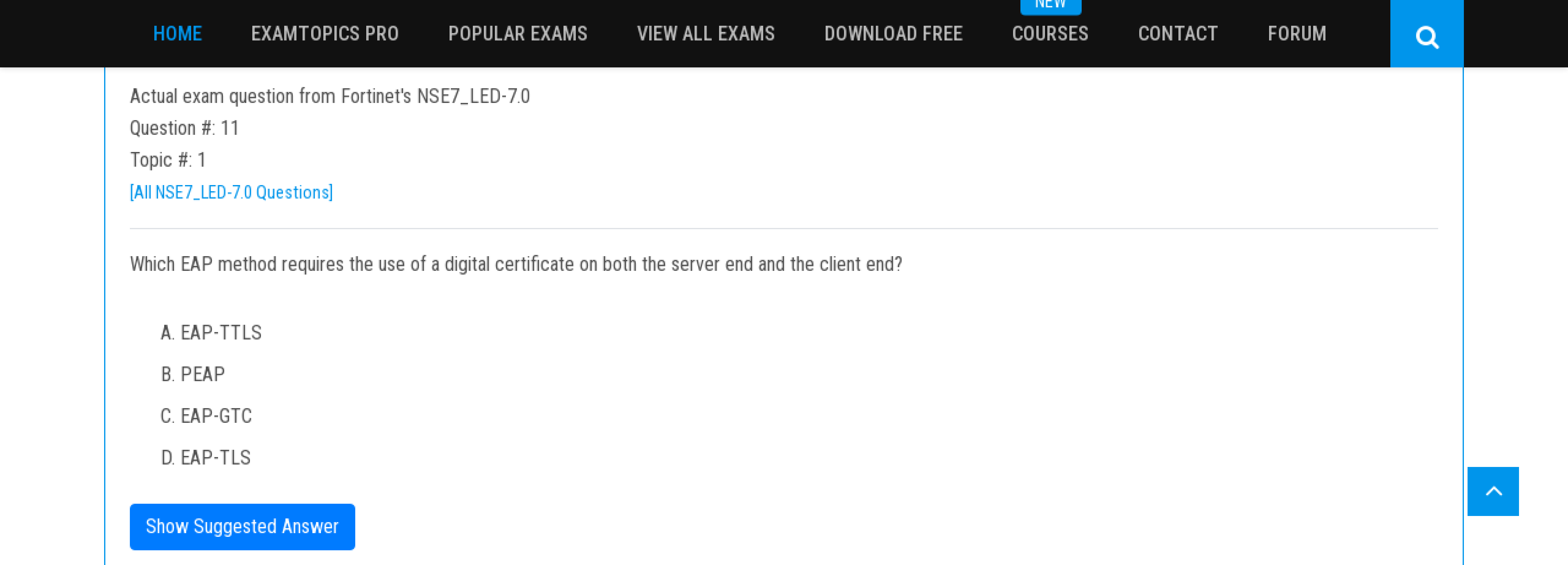
A. Configure split-tunneling in the vap configuration.

B. Configure split-tunneling in the wtp-profile configuration.

C. Disable the Block Intra-SSID Traffic (Intra-vap-privacy) setting on the SSID (VAP) profile.

D. Configure the printer as a wireless client on the Corporate wireless network.

Show Suggested Answer



Actual exam question from Fortinet's NSE7_LED-7.0

Question #: 11

Topic #: 1

[All NSE7_LED-7.0 Questions]

Which EAP method requires the use of a digital certificate on both the server end and the client end?

A. EAP-TTLS

B. PEAP

C. EAP-GTC

D. EAP-TLS

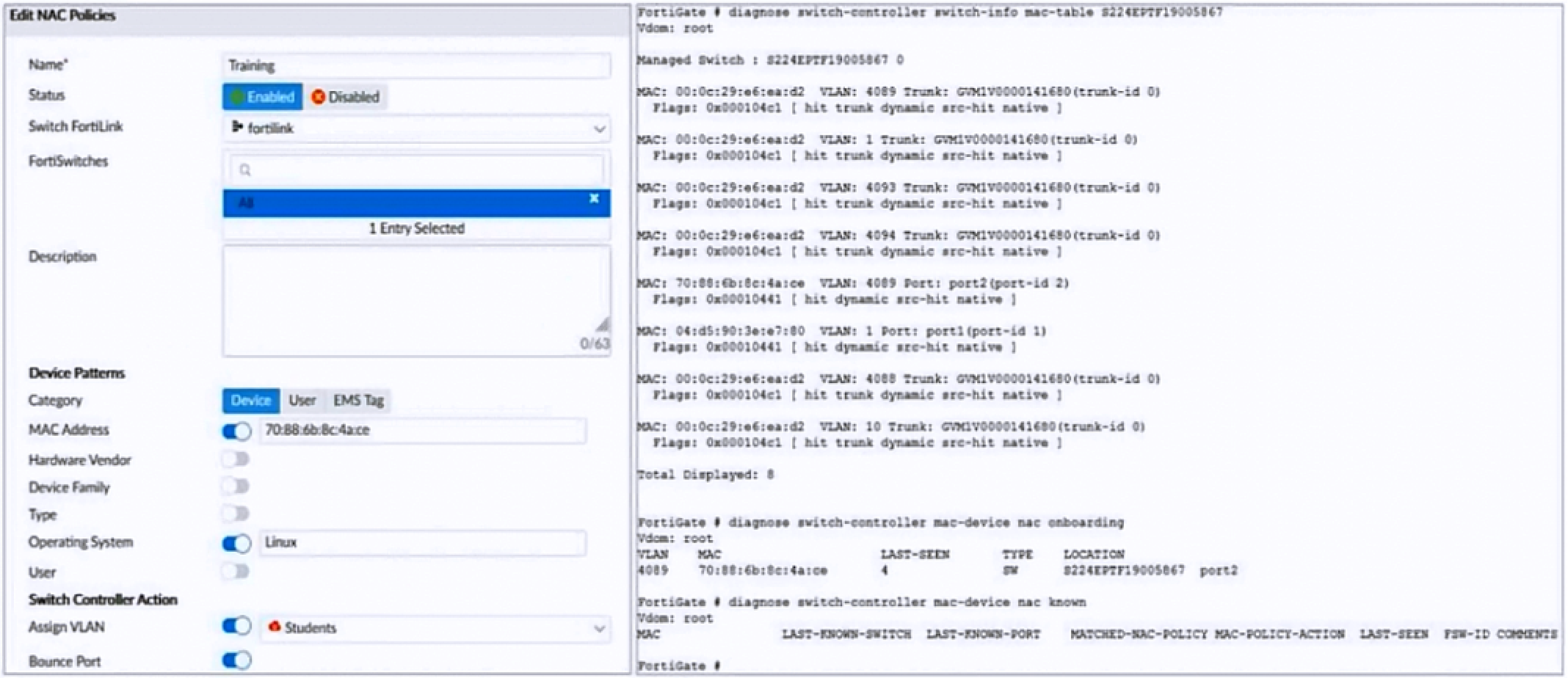
Actual exam question from Fortinet's NSE7_LED-7.0

Question #: 12

Topic #: 1

[All NSE7_LED-7.0 Questions]

Refer to the exhibit.



Edit NAC Policies

Name* Training

Status ● Enabled ○ Disabled

Switch FortiLink fortilink

FortiSwitches All — 1 Entry Selected

Description 0/63

Device Patterns

Category: Device | User | EMS Tag

MAC Address ● 70:88:6b:8c:4a:ce

Hardware Vendor ○

Device Family ○

Type ○

Operating System ● Linux

User ○

Switch Controller Action

Assign VLAN ● Students

Bounce Port ●

```
FortiGate # diagnose switch-controller switch-info mac-table S224EPTF19005867
Vdom: root

Managed Switch : S224EPTF19005867 0

MAC: 00:0c:29:e6:ea:d2  VLAN: 4089 Trunk: GVM1V0000141680(trunk-id 0)
  Flags: 0x000104c1 [ hit trunk dynamic src-hit native ]

MAC: 00:0c:29:e6:ea:d2  VLAN: 1 Trunk: GVM1V0000141680(trunk-id 0)
  Flags: 0x000104c1 [ hit trunk dynamic src-hit native ]

MAC: 00:0c:29:e6:ea:d2  VLAN: 4093 Trunk: GVM1V0000141680(trunk-id 0)
  Flags: 0x000104c1 [ hit trunk dynamic src-hit native ]

MAC: 00:0c:29:e6:ea:d2  VLAN: 4094 Trunk: GVM1V0000141680(trunk-id 0)
  Flags: 0x000104c1 [ hit trunk dynamic src-hit native ]

MAC: 70:88:6b:8c:4a:ce  VLAN: 4089 Port: port2(port-id 2)
  Flags: 0x00010441 [ hit dynamic src-hit native ]

MAC: 04:d5:90:3e:e7:80  VLAN: 1 Port: port1(port-id 1)
  Flags: 0x00010441 [ hit dynamic src-hit native ]

MAC: 00:0c:29:e6:ea:d2  VLAN: 4088 Trunk: GVM1V0000141680(trunk-id 0)
  Flags: 0x000104c1 [ hit trunk dynamic src-hit native ]

MAC: 00:0c:29:e6:ea:d2  VLAN: 10 Trunk: GVM1V0000141680(trunk-id 0)
  Flags: 0x000104c1 [ hit trunk dynamic src-hit native ]

Total Displayed: 8


FortiGate # diagnose switch-controller mac-device nac onboarding
Vdom: root
VLAN    MAC                    LAST-SEEN      TYPE    LOCATION
4089    70:88:6b:8c:4a:ce      4              SW      S224EPTF19005867  port2

FortiGate # diagnose switch-controller mac-device nac known
Vdom: root
MAC                  LAST-KNOWN-SWITCH  LAST-KNOWN-PORT   MATCHED-NAC-POLICY MAC-POLICY-ACTION  LAST-SEEN  FSW-ID COMMENTS

FortiGate #
```

Examine the FortiManager configuration and FortiGate CLI output shown in the exhibit.

An administrator is testing the NAC feature. The test device is connected to a managed FortiSwitch device (S224EPTF19005867) on port2.

After applying the NAC policy on port2 and generating traffic on the test device, the test device is not matching the NAC policy; therefore, the test device remains in the onboarding VLAN.

Based on the information shown in the exhibit, which two scenarios are likely to cause this issue? (Choose two.)

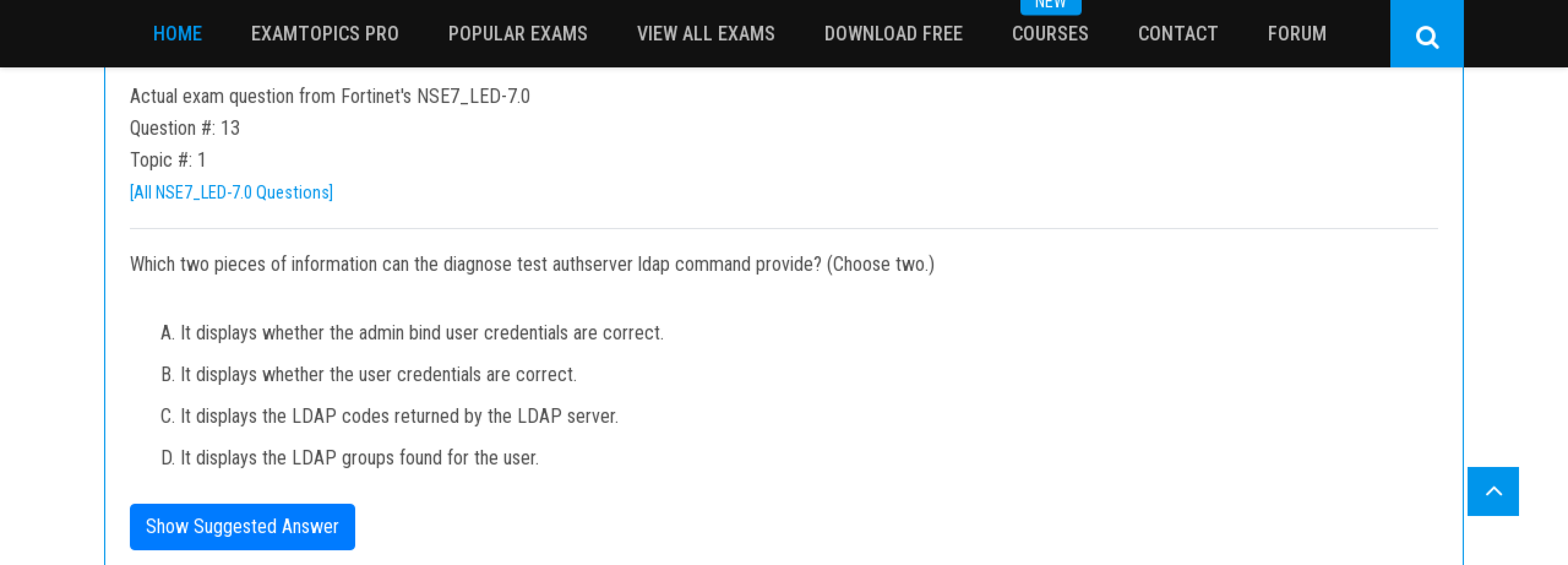
A. Management communication between FortiGate and FortiSwitch is down.

B. The MAC address configured on the NAC policy is incorrect.

C. The device operating system detected by FortiGate is not Linux.

D. Device detection is not enabled on VLAN 4089.

Show Suggested Answer



Actual exam question from Fortinet's NSE7_LED-7.0

Question #: 13

Topic #: 1

[All NSE7_LED-7.0 Questions]

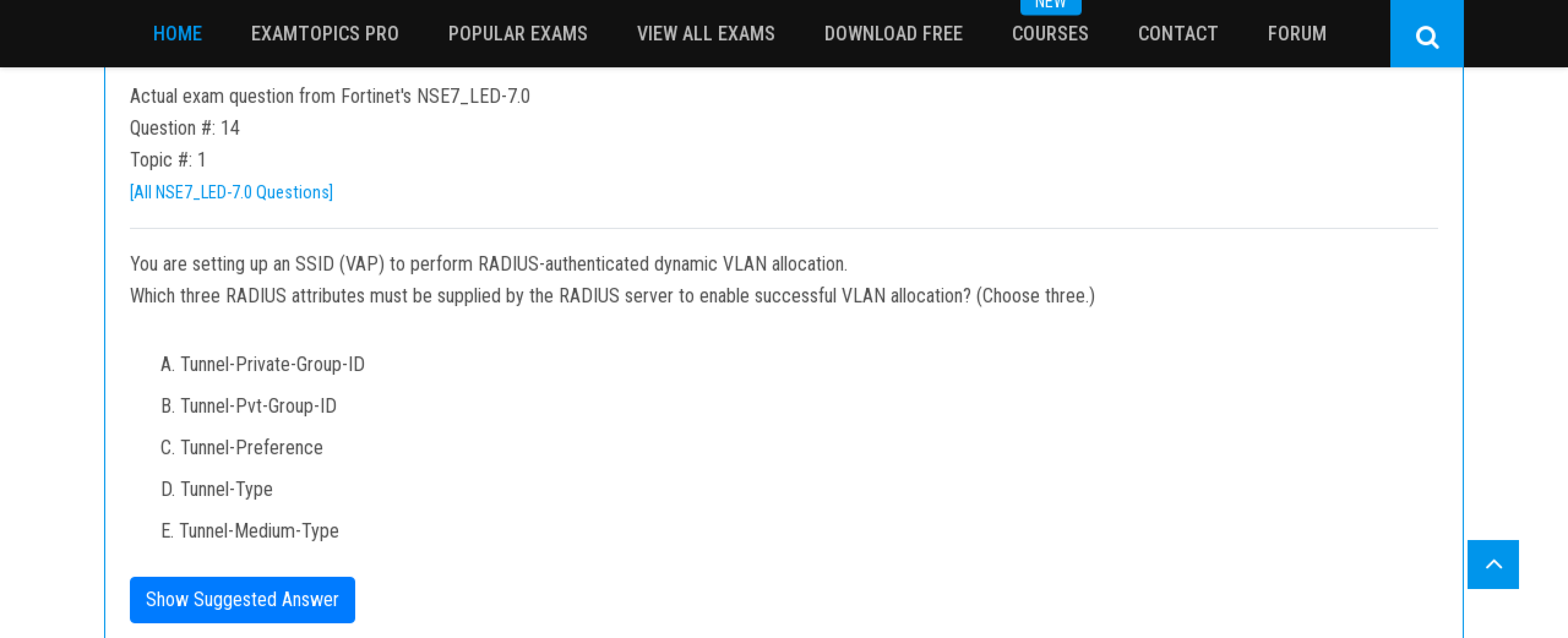
Which two pieces of information can the diagnose test authserver ldap command provide? (Choose two.)

A. It displays whether the admin bind user credentials are correct.

B. It displays whether the user credentials are correct.

C. It displays the LDAP codes returned by the LDAP server.

D. It displays the LDAP groups found for the user.



Actual exam question from Fortinet's NSE7_LED-7.0

Question #: 14

Topic #: 1

[All NSE7_LED-7.0 Questions]

You are setting up an SSID (VAP) to perform RADIUS-authenticated dynamic VLAN allocation.

Which three RADIUS attributes must be supplied by the RADIUS server to enable successful VLAN allocation? (Choose three.)

A. Tunnel-Private-Group-ID

B. Tunnel-Pvt-Group-ID

C. Tunnel-Preference

D. Tunnel-Type

E. Tunnel-Medium-Type

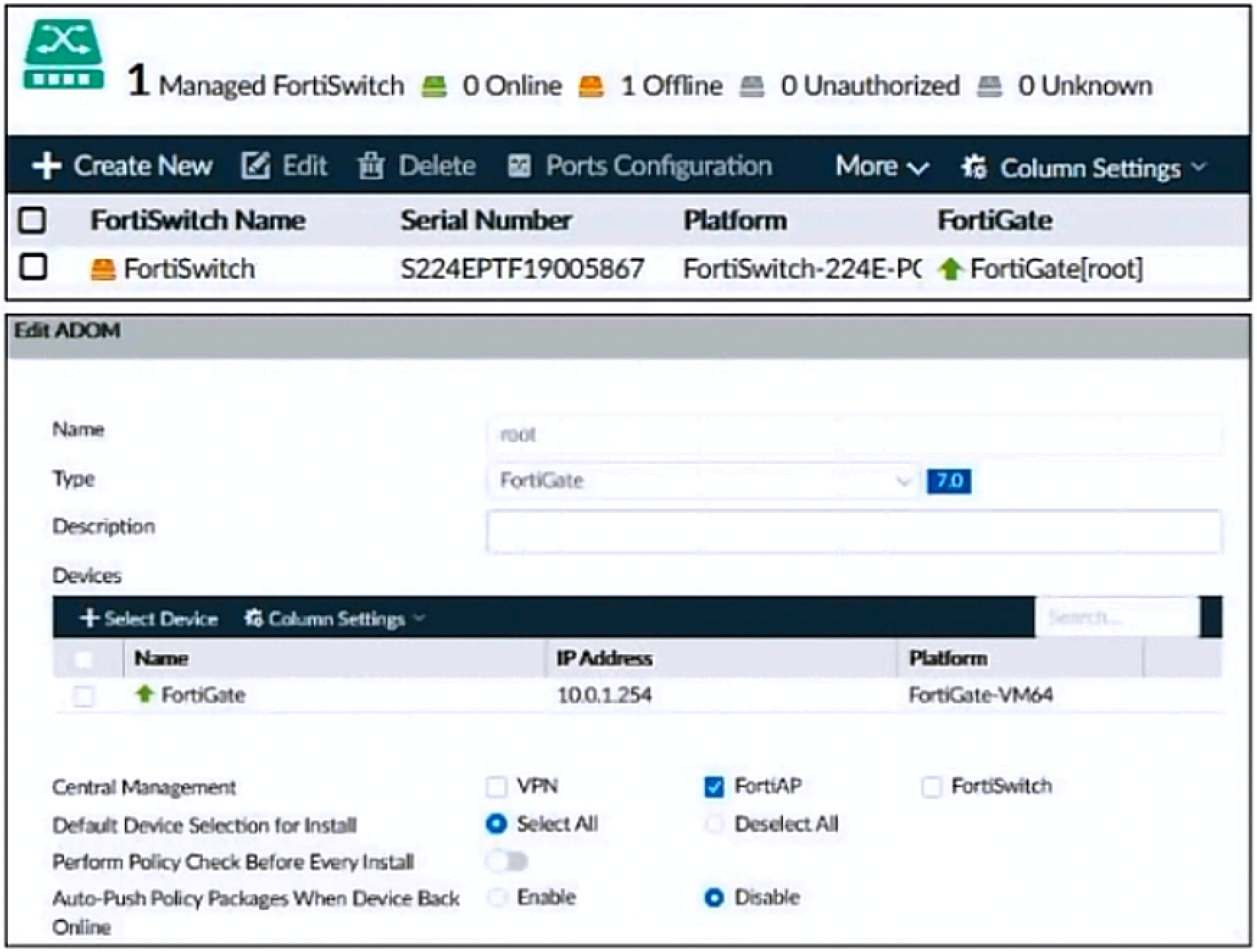
Actual exam question from Fortinet's NSE7_LED-7.0

Question #: 15

Topic #: 1

[All NSE7_LED-7.0 Questions]

Refer to the exhibit.



1 Managed FortiSwitch 0 Online 1 Offline 0 Unauthorized 0 Unknown

□	FortiSwitch Name	Serial Number	Platform	FortiGate
□	FortiSwitch	S224EPTF19005867	FortiSwitch-224E-PC	FortiGate[root]

Edit ADOM

Name: root

Type: FortiGate 7.0

Description:

Devices

□	Name	IP Address	Platform
□	FortiGate	10.0.1.254	FortiGate-VM64

Central Management: □ VPN ☑ FortiAP □ FortiSwitch

Default Device Selection for Install: ● Select All ○ Deselect All

Perform Policy Check Before Every Install: (off)

Auto-Push Policy Packages When Device Back Online: ○ Enable ● Disable

Examine the FortiManager information shown in the exhibit.

Which two statements about the FortiManager status are true? (Choose two.)

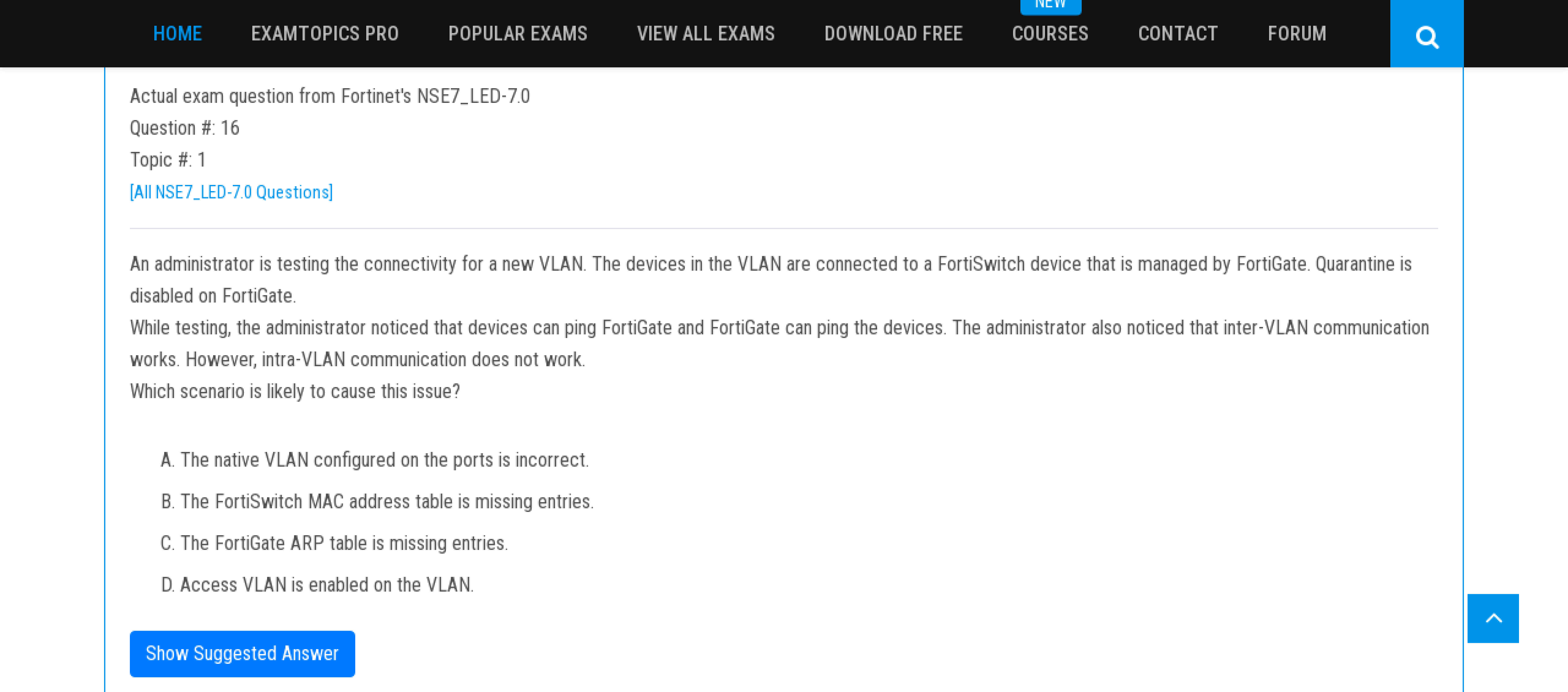
A. FortiSwitch manager is working in per-device management mode.

B. FortiSwitch is not authorized.

C. FortiSwitch manager is working in central management mode.

D. FortiSwitch is authorized and offline.

Show Suggested Answer



Actual exam question from Fortinet's NSE7_LED-7.0

Question #: 16

Topic #: 1

[All NSE7_LED-7.0 Questions]

An administrator is testing the connectivity for a new VLAN. The devices in the VLAN are connected to a FortiSwitch device that is managed by FortiGate. Quarantine is disabled on FortiGate.

While testing, the administrator noticed that devices can ping FortiGate and FortiGate can ping the devices. The administrator also noticed that inter-VLAN communication works. However, intra-VLAN communication does not work.

Which scenario is likely to cause this issue?

A. The native VLAN configured on the ports is incorrect.

B. The FortiSwitch MAC address table is missing entries.

C. The FortiGate ARP table is missing entries.

D. Access VLAN is enabled on the VLAN.

Show Suggested Answer

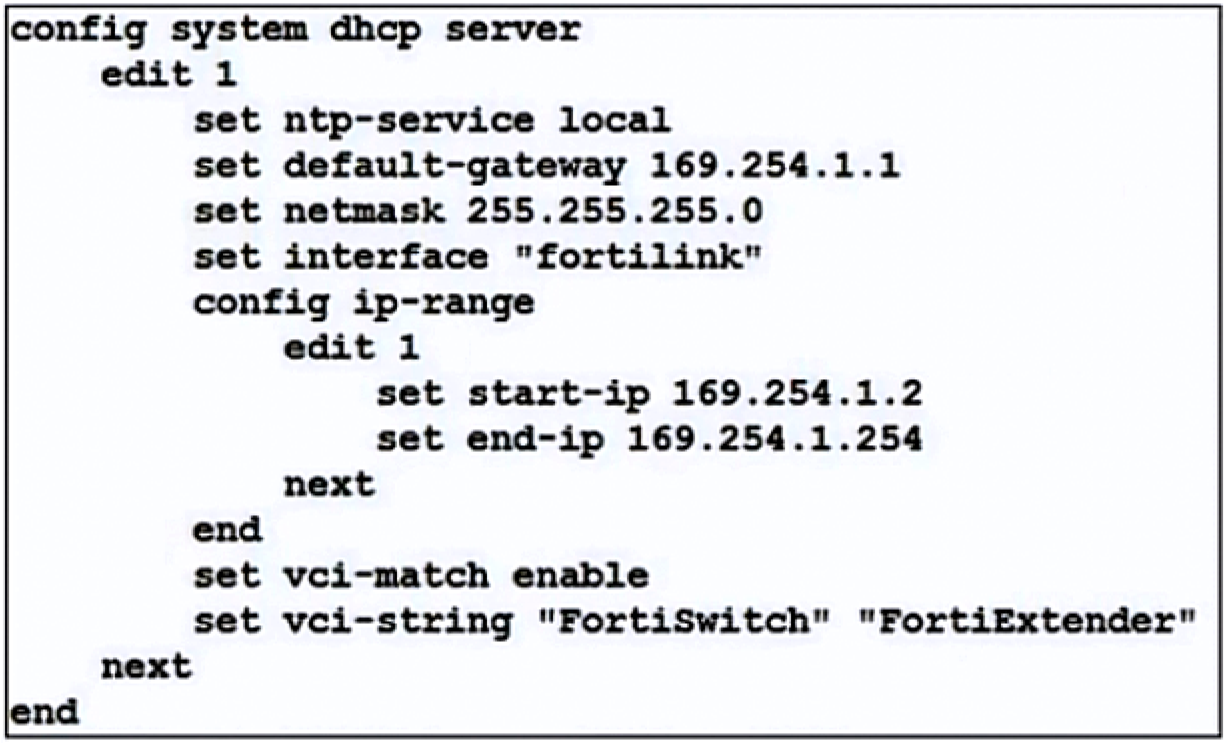
Actual exam question from Fortinet's NSE7_LED-7.0

Question #: 17

Topic #: 1

[All NSE7_LED-7.0 Questions]

Refer to the exhibit.



```
config system dhcp server
    edit 1
        set ntp-service local
        set default-gateway 169.254.1.1
        set netmask 255.255.255.0
        set interface "fortilink"
        config ip-range
            edit 1
                set start-ip 169.254.1.2
                set end-ip 169.254.1.254
            next
        end
        set vci-match enable
        set vci-string "FortiSwitch" "FortiExtender"
    next
end
```

By default, FortiOS creates the following DHCP server scope for the FortiLink interface as shown in the exhibit.

What is the objective of the vci-string setting?

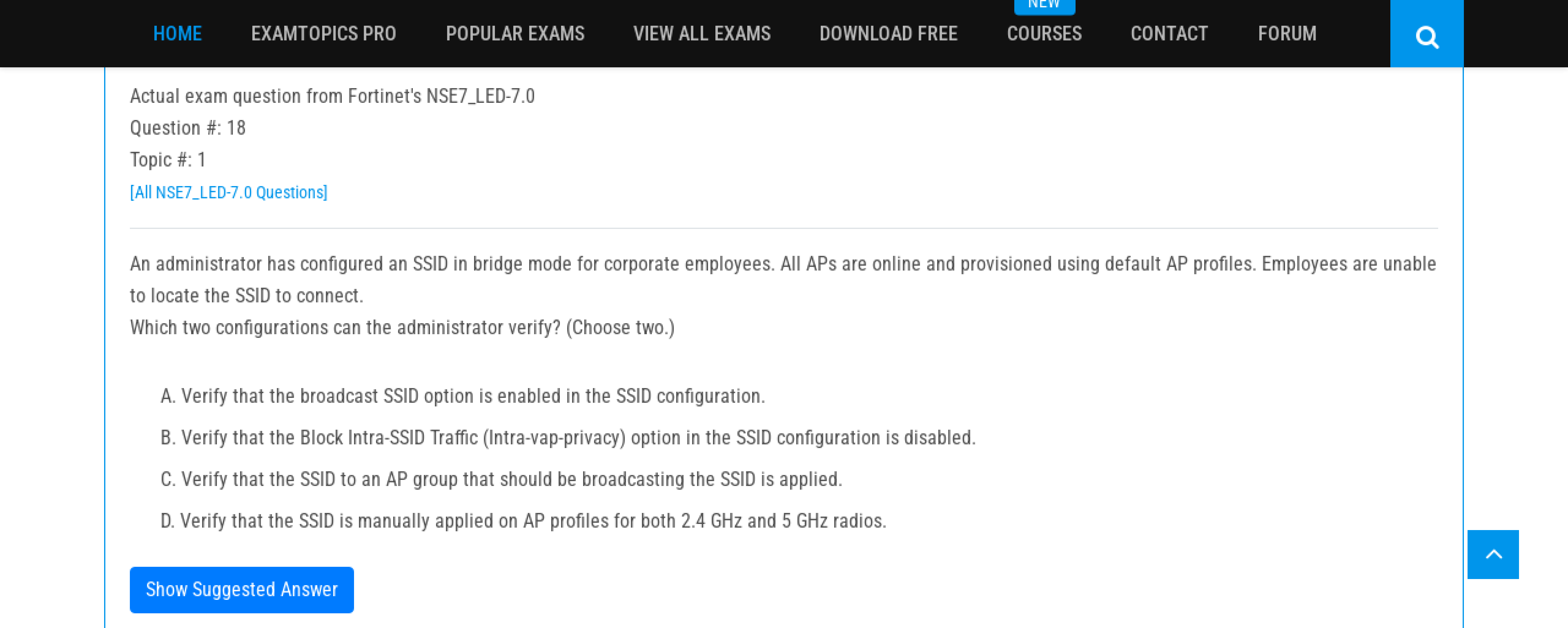
A. To ignore DHCP requests coming from FortiSwitch and FortiExtender devices

B. To reserve IP addresses for FortiSwitch and FortiExtender devices

C. To restrict the IP address assignment to FortiSwitch and FortiExtender devices

D. To restrict the IP address assignment to devices that have FortiSwitch or FortiExtender as their hostname

Show Suggested Answer



Actual exam question from Fortinet's NSE7_LED-7.0

Question #: 18

Topic #: 1

[All NSE7_LED-7.0 Questions]

An administrator has configured an SSID in bridge mode for corporate employees. All APs are online and provisioned using default AP profiles. Employees are unable to locate the SSID to connect.

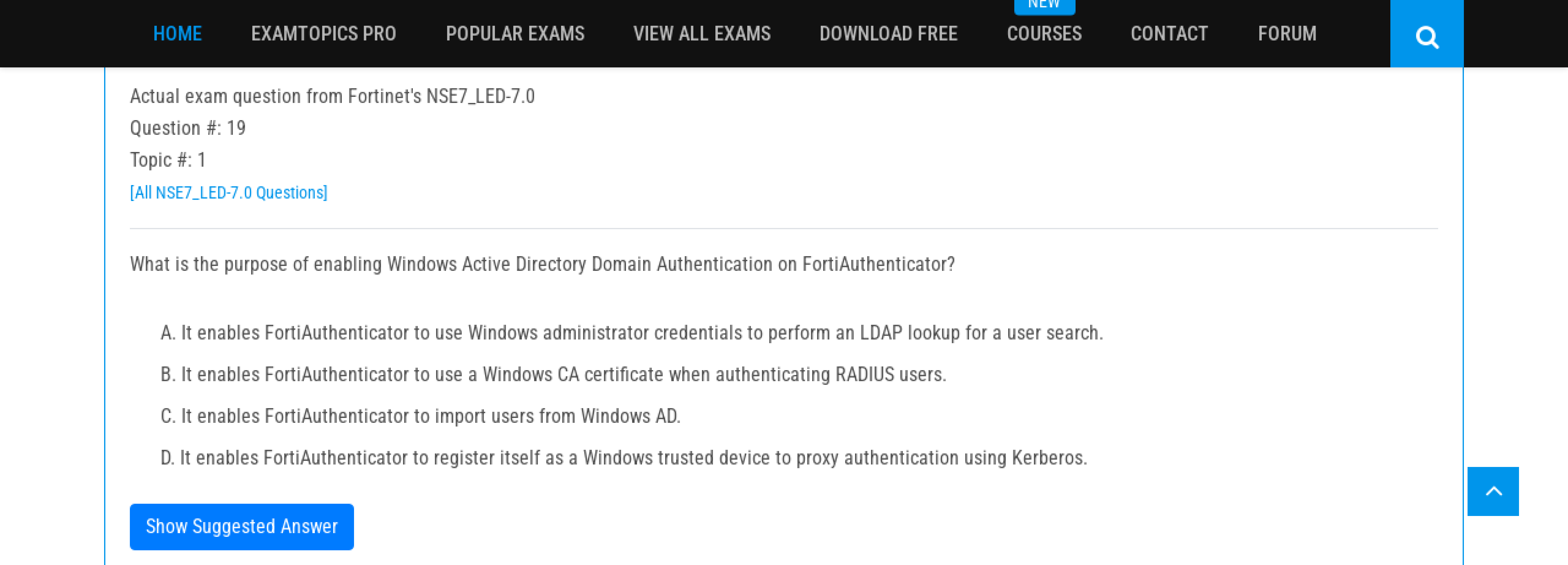
Which two configurations can the administrator verify? (Choose two.)

A. Verify that the broadcast SSID option is enabled in the SSID configuration.

B. Verify that the Block Intra-SSID Traffic (Intra-vap-privacy) option in the SSID configuration is disabled.

C. Verify that the SSID to an AP group that should be broadcasting the SSID is applied.

D. Verify that the SSID is manually applied on AP profiles for both 2.4 GHz and 5 GHz radios.



Actual exam question from Fortinet's NSE7_LED-7.0

Question #: 19

Topic #: 1

[All NSE7_LED-7.0 Questions]

What is the purpose of enabling Windows Active Directory Domain Authentication on FortiAuthenticator?

A. It enables FortiAuthenticator to use Windows administrator credentials to perform an LDAP lookup for a user search.

B. It enables FortiAuthenticator to use a Windows CA certificate when authenticating RADIUS users.

C. It enables FortiAuthenticator to import users from Windows AD.

D. It enables FortiAuthenticator to register itself as a Windows trusted device to proxy authentication using Kerberos.

Show Suggested Answer

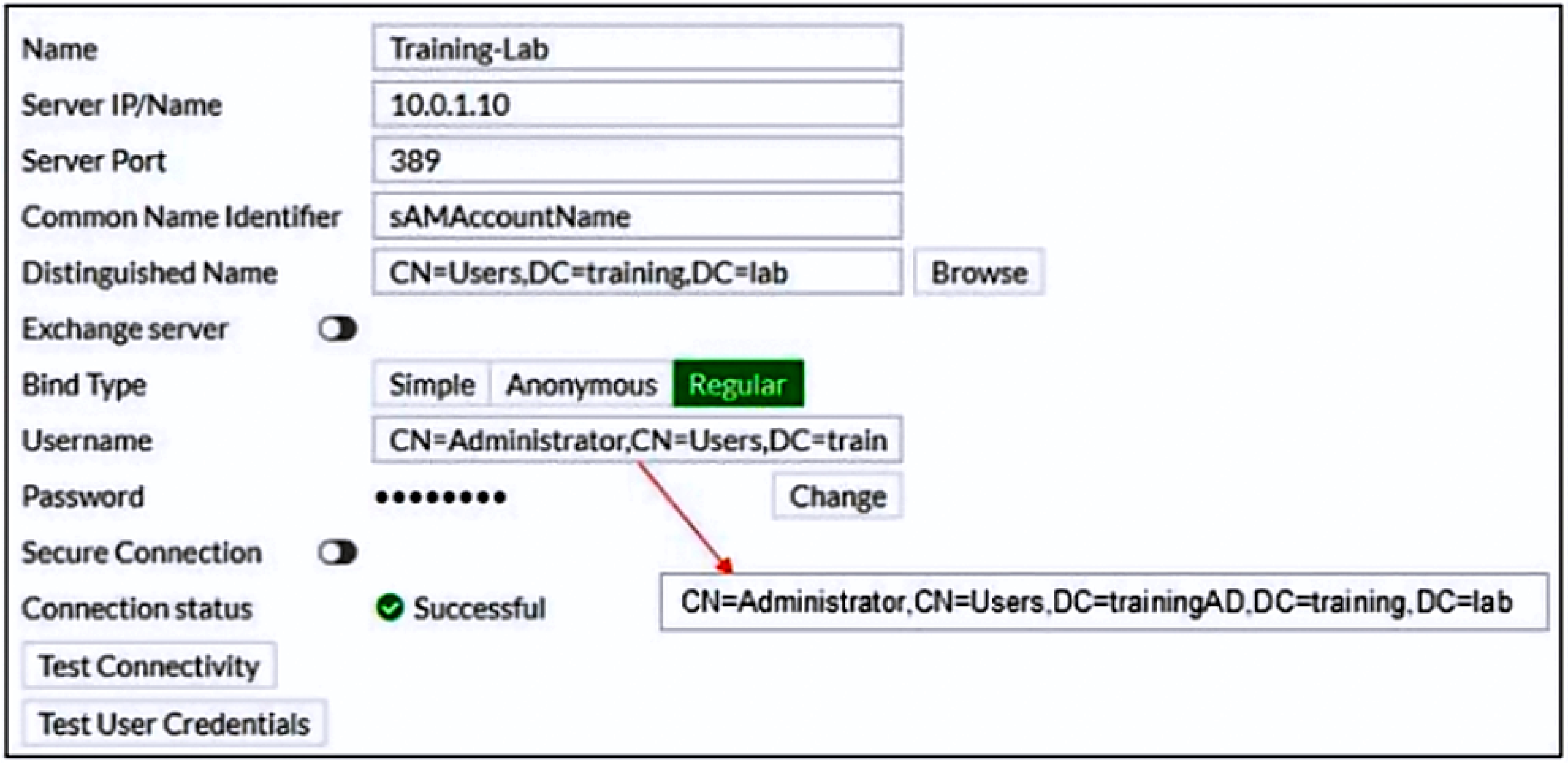
Actual exam question from Fortinet's NSE7_LED-7.0

Question #: 20

Topic #: 1

[All NSE7_LED-7.0 Questions]

Refer to the exhibit.



Name	Training-Lab	
Server IP/Name	10.0.1.10	
Server Port	389	
Common Name Identifier	sAMAccountName	
Distinguished Name	CN=Users,DC=training,DC=lab	Browse
Exchange server	○	
Bind Type	Simple Anonymous [✓ Regular]	
Username	CN=Administrator,CN=Users,DC=train	
Password	••••••••	Change
Secure Connection	○	
Connection status	✓ Successful	
Test Connectivity		
Test User Credentials		

CN=Administrator,CN=Users,DC=trainingAD,DC=training,DC=lab

Examine the LDAP server configuration shown in the exhibit. Note that the Username setting has been expanded to display its full content.

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

```
>dsquery user -samid student
"CN=student,CN=Users,DC=trainingAD,DC=training,DC=lab"
```

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

A. Common Name Identifier

B. Bind Type

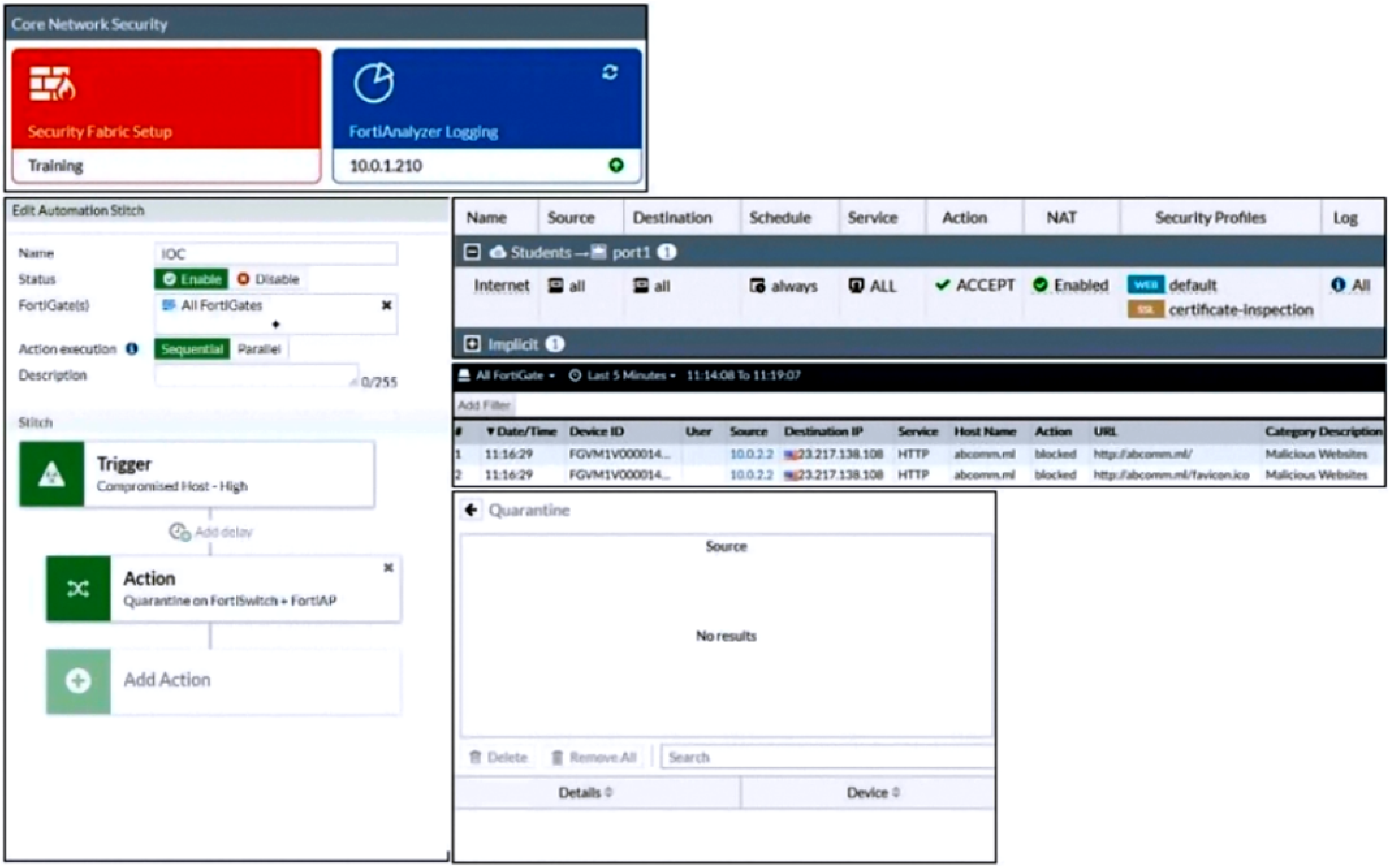
C. Distinguished Name

D. Username

Show Suggested Answer

Actual exam question from Fortinet's NSE7_LED-7.0
Question #: 21
Topic #: 1
[All NSE7_LED-7.0 Questions]

Refer to the exhibit.



Core Network Security

Security Fabric Setup: Training

FortiAnalyzer Logging: 10.0.1.210

Edit Automation Stitch

Name: IOC
Status: Enable | Disable
FortiGate(s): All FortiGates
Action execution: Sequential | Parallel
Description: 0/255

Stitch

Trigger: Compromised Host - High

Add delay

Action: Quarantine on FortiSwitch + FortiAP

Add Action

Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log
Students → port1 1								
Internet	all	all	always	ALL	✓ ACCEPT	Enabled	WEB default SSL certificate-inspection	All
Implicit 1								

All FortiGate ▾ Last 5 Minutes ▾ 11:14:08 To 11:19:07

Add Filter

#	▾Date/Time	Device ID	User	Source	Destination IP	Service	Host Name	Action	URL	Category Description
1	11:16:29	FGVM1V000014...		10.0.2.2	23.217.138.108	HTTP	abcomm.ml	blocked	http://abcomm.ml/	Malicious Websites
2	11:16:29	FGVM1V000014...		10.0.2.2	23.217.138.108	HTTP	abcomm.ml	blocked	http://abcomm.ml/favicon.ico	Malicious Websites

Quarantine

Source

No results

Delete Remove All Search

Details	Device

Examine the FortiGate configuration, FortiAnalyzer logs, and FortiGate widget shown in the exhibit.
An administrator is testing the Security Fabric quarantine automation. The administrator added FortiAnalyzer to the Security Fabric, and configured an automation stitch to automatically quarantine compromised devices. The test device (10.0.2.1) is connected to a managed FortiSwitch device.
After trying to access a malicious website from the test device, the administrator verifies that FortiAnalyzer has a log for the test connection. However, the device is not getting quarantined by FortiGate, as shown in the quarantine widget.
Which two scenarios are likely to cause this issue? (Choose two.)

A. The web filtering rating service is not working.

B. FortiAnalyzer does not have a valid threat detection services license.

C. The device does not have FortiClient installed.

D. FortiAnalyzer does not consider the malicious website an indicator of compromise (IOC).

Show Suggested Answer

Actual exam question from Fortinet's NSE7_LED-7.0

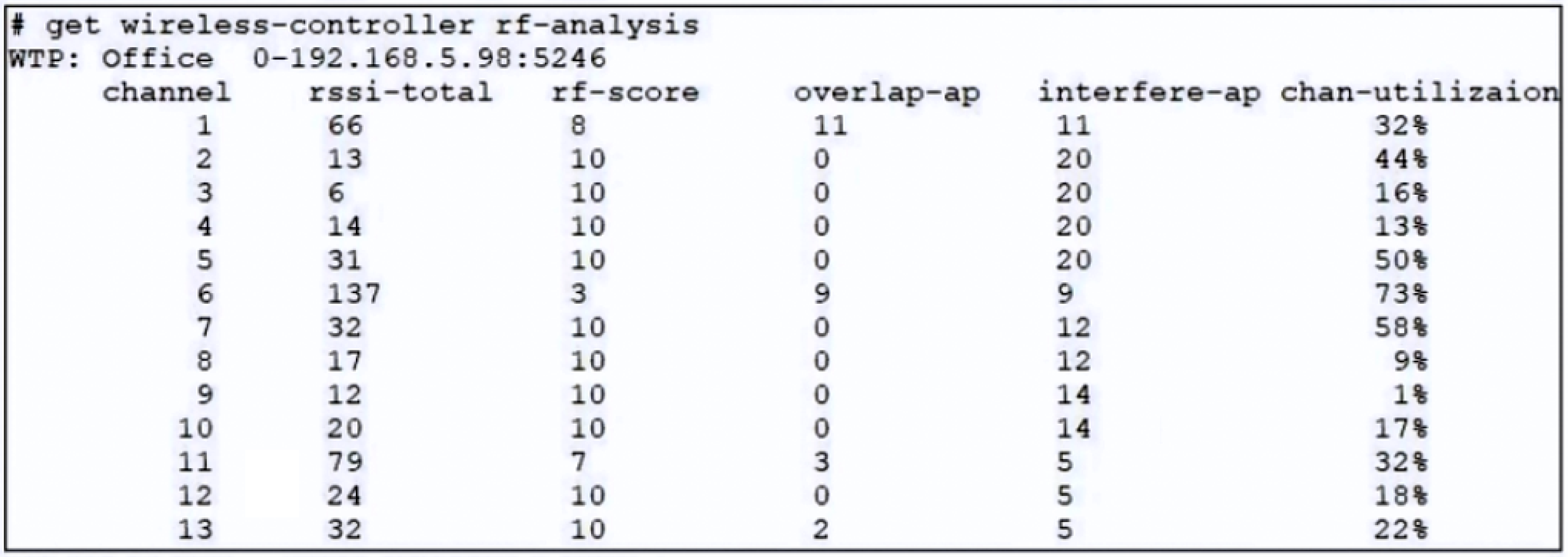
Question #: 22

Topic #: 1

[All NSE7_LED-7.0 Questions]

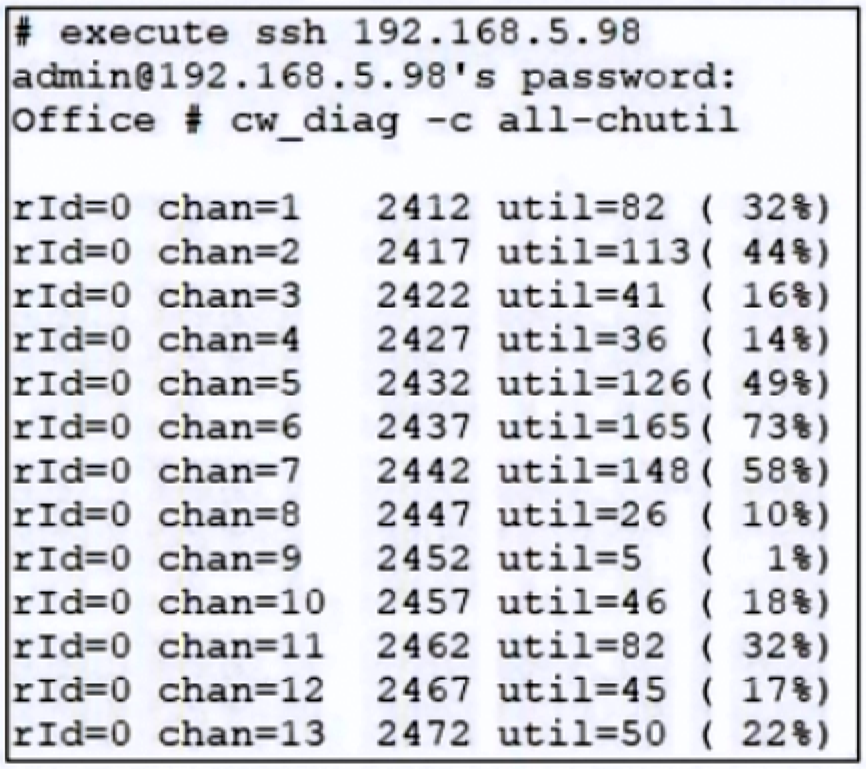
Refer to the exhibits.

Exhibit



```
# get wireless-controller rf-analysis
WTP: Office  0-192.168.5.98:5246
     channel     rssi-total  rf-score     overlap-ap   interfere-ap chan-utilizaion
          1        66          8            11           11               32%
          2        13          10           0            20               44%
          3        6           10           0            20               16%
          4        14          10           0            20               13%
          5        31          10           0            20               50%
          6        137         3            9            9                73%
          7        32          10           0            12               58%
          8        17          10           0            12                9%
          9        12          10           0            14                1%
         10        20          10           0            14               17%
         11        79          7            3            5                32%
         12        24          10           0            5                18%
         13        32          10           2            5                22%
```

Exhibit



```
# execute ssh 192.168.5.98
admin@192.168.5.98's password:
Office # cw_diag -c all-chutil

rId=0 chan=1   2412 util=82  ( 32%)
rId=0 chan=2   2417 util=113( 44%)
rId=0 chan=3   2422 util=41  ( 16%)
rId=0 chan=4   2427 util=36  ( 14%)
rId=0 chan=5   2432 util=126( 49%)
rId=0 chan=6   2437 util=165( 73%)
rId=0 chan=7   2442 util=148( 58%)
rId=0 chan=8   2447 util=26  ( 10%)
rId=0 chan=9   2452 util=5   (  1%)
rId=0 chan=10  2457 util=46  ( 18%)
rId=0 chan=11  2462 util=82  ( 32%)
rId=0 chan=12  2467 util=45  ( 17%)
rId=0 chan=13  2472 util=50  ( 22%)
```

Examine the troubleshooting outputs shown in the exhibits.

Users have been reporting issues with the speed of their wireless connection in a particular part of the wireless network. The interface that is having issues is the 2.4 GHz interface that is currently configured on channel 6.

The administrator of the wireless network has investigated and surveyed the local RF environment using the tools available at the AP and FortiGate.

Which configuration would improve the wireless connection?

A. Change the AP 2.4 GHz channel to 11

B. Change the AP 2.4 GHz channel to 1

C. Change the AP 2.4 GHz channel to 9.

D. Change the AP 2.4 GHz channel to 13.

Show Suggested Answer

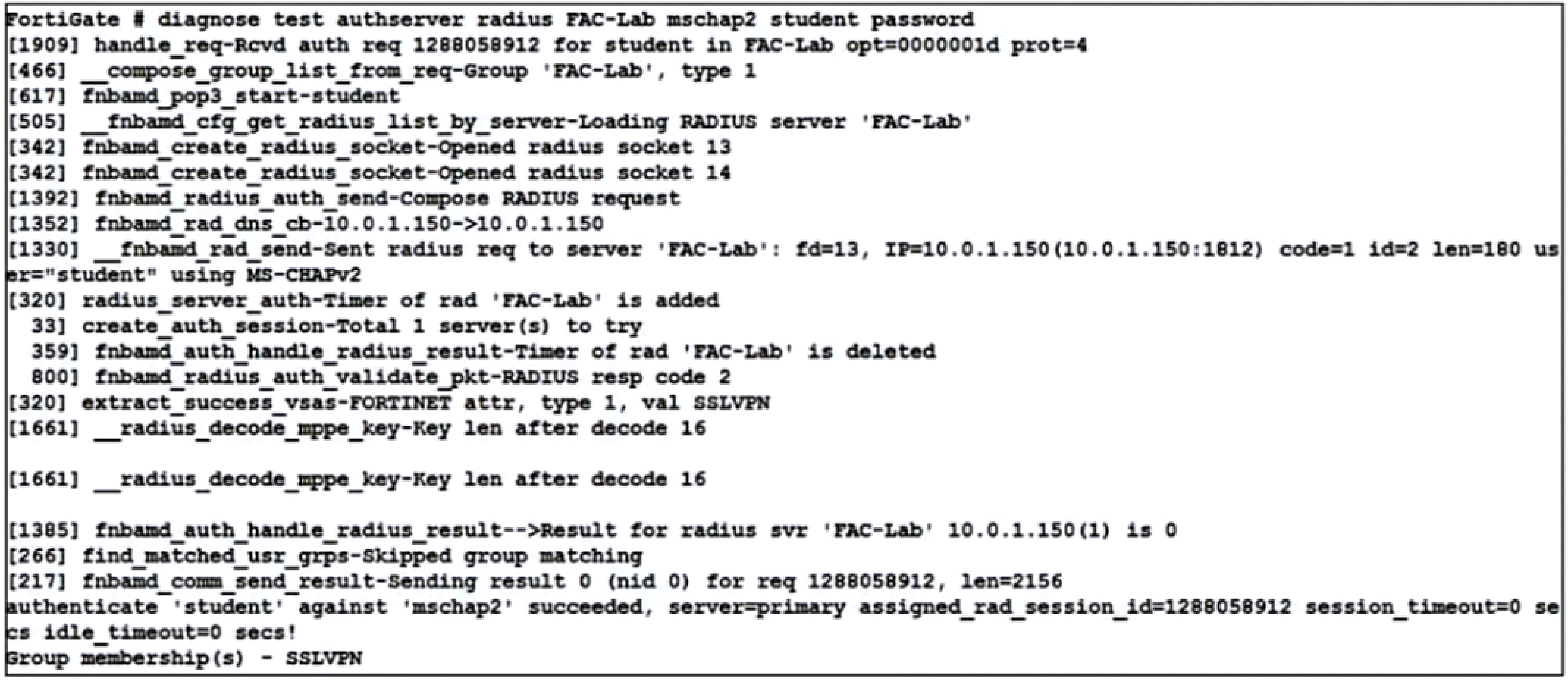
Actual exam question from Fortinet's NSE7_LED-7.0

Question #: 23

Topic #: 1

[All NSE7_LED-7.0 Questions]

Refer to the exhibit.



```
FortiGate # diagnose test authserver radius FAC-Lab mschap2 student password
[1909] handle_req-Rcvd auth req 1288058912 for student in FAC-Lab opt=0000001d prot=4
[466] __compose_group_list_from_req-Group 'FAC-Lab', type 1
[617] fnbamd_pop3_start-student
[505] __fnbamd_cfg_get_radius_list_by_server-Loading RADIUS server 'FAC-Lab'
[342] fnbamd_create_radius_socket-Opened radius socket 13
[342] fnbamd_create_radius_socket-Opened radius socket 14
[1392] fnbamd_radius_auth_send-Compose RADIUS request
[1352] fnbamd_rad_dns_cb-10.0.1.150->10.0.1.150
[1330] __fnbamd_rad_send-Sent radius req to server 'FAC-Lab': fd=13, IP=10.0.1.150(10.0.1.150:1812) code=1 id=2 len=180 us
er="student" using MS-CHAPv2
[320] radius_server_auth-Timer of rad 'FAC-Lab' is added
  33] create_auth_session-Total 1 server(s) to try
  359] fnbamd_auth_handle_radius_result-Timer of rad 'FAC-Lab' is deleted
  800] fnbamd_radius_auth_validate_pkt-RADIUS resp code 2
[320] extract_success_vsas-FORTINET attr, type 1, val SSLVPN
[1661] __radius_decode_mppe_key-Key len after decode 16

[1661] __radius_decode_mppe_key-Key len after decode 16

[1385] fnbamd_auth_handle_radius_result-->Result for radius svr 'FAC-Lab' 10.0.1.150(1) is 0
[266] find_matched_usr_grps-Skipped group matching
[217] fnbamd_comm_send_result-Sending result 0 (nid 0) for req 1288058912, len=2156
authenticate 'student' against 'mschap2' succeeded, server=primary assigned_rad_session_id=1288058912 session_timeout=0 se
cs idle_timeout=0 secs!
Group membership(s) - SSLVPN
```

Examine the debug output shown in the exhibit.

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

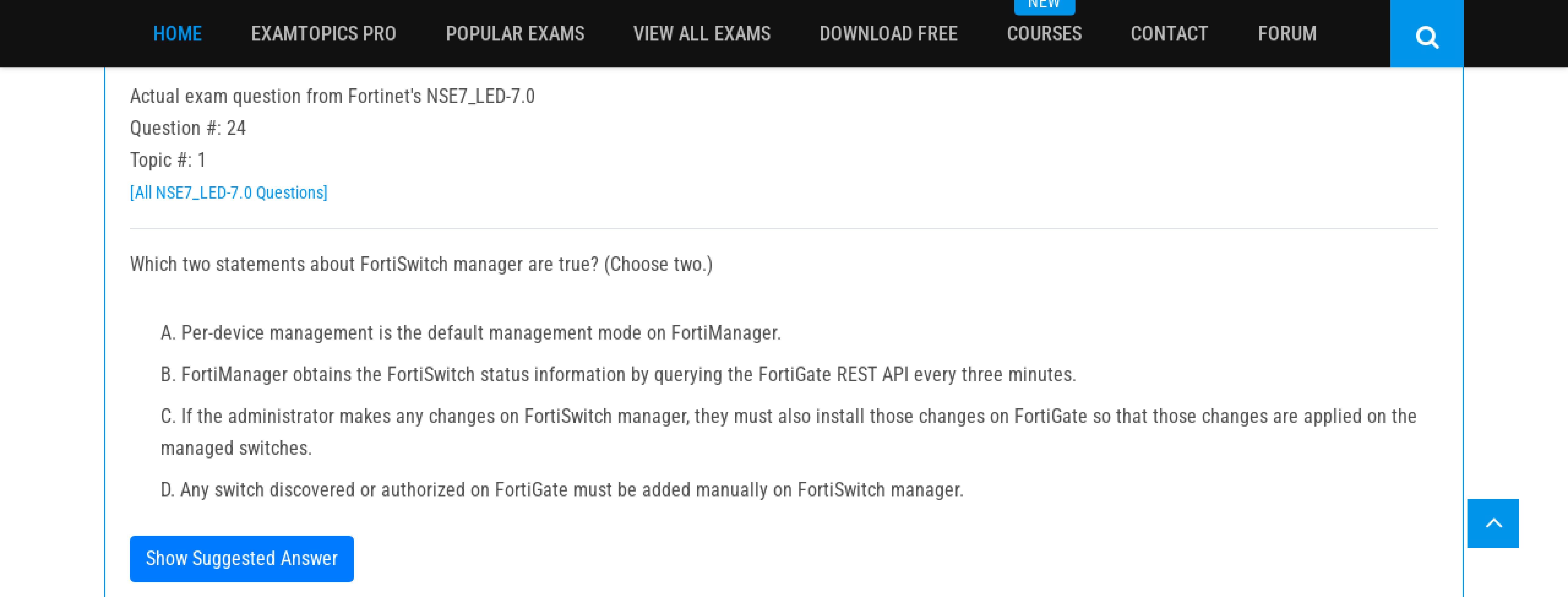
A. The user student belongs to the SSLVPN group.

B. User authentication failed.

C. The RADIUS server sent a vendor-specific attribute in the RADIUS response.

D. User authentication succeeded using MSCHAP.

Show Suggested Answer



Actual exam question from Fortinet's NSE7_LED-7.0

Question #: 24

Topic #: 1

[All NSE7_LED-7.0 Questions]

Which two statements about FortiSwitch manager are true? (Choose two.)

A. Per-device management is the default management mode on FortiManager.

B. FortiManager obtains the FortiSwitch status information by querying the FortiGate REST API every three minutes.

C. If the administrator makes any changes on FortiSwitch manager, they must also install those changes on FortiGate so that those changes are applied on the managed switches.

D. Any switch discovered or authorized on FortiGate must be added manually on FortiSwitch manager.

Show Suggested Answer