Fortinet

Exam Questions FCSS_LED_AR-7.6

FCSS - LAN Edge 7.6 Architect

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

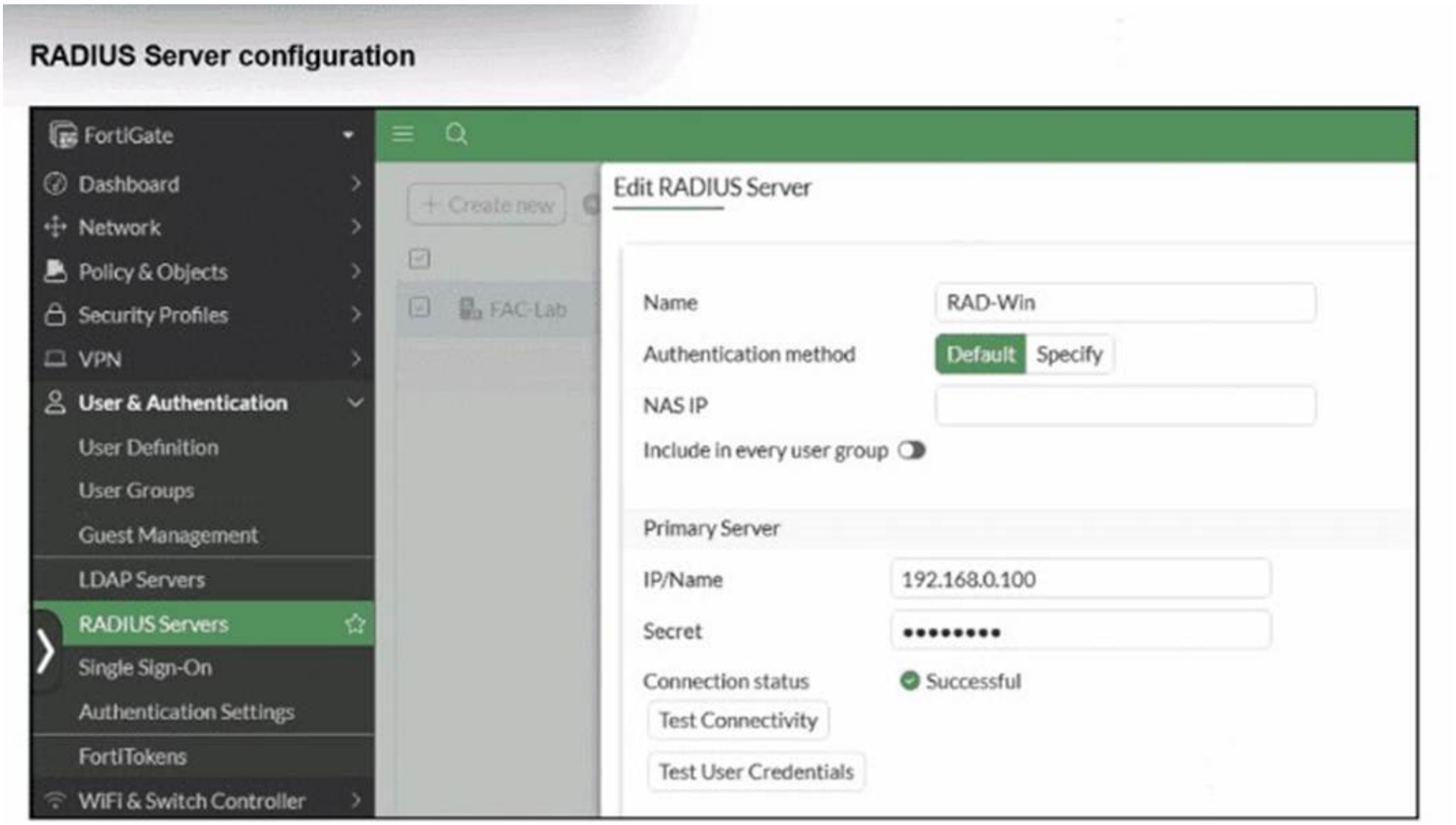
If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1
Which FortiGuard licenses are required for FortiLink device detection to enable device identification and vulnerability detection?

A. FortiGuard Vulnerability Management and FortiGuard Endpoit Protection
B. FortiGuard Threat Intelligence and FortiGuard loT Detection
C. FortiGuard Threat Intelligence and FortiGuard Endpoint Protection
D. FortiGuard Attack Surface Security and FortiGuard loT Detection

Answer: D

NEW QUESTION 2
Refer to the exhibit.



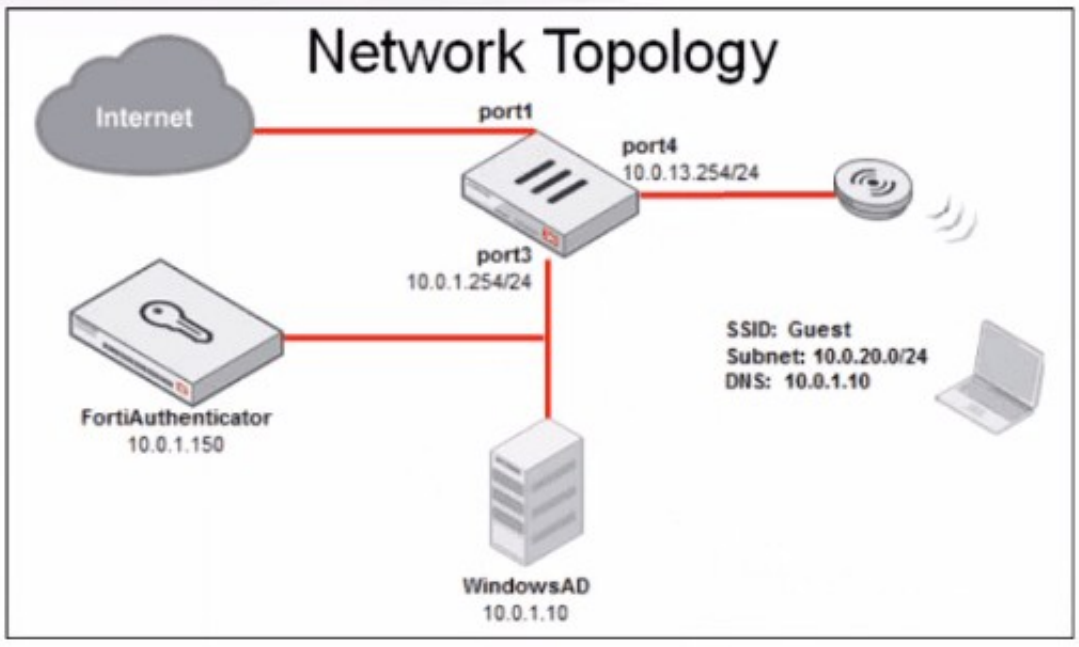
On FortiGate, a RADIUS server is configured to forward authentication requests to FortiAuthenticator, which acts as a RADIUS proxy. FortiAuthenticator then relays these authentication requests to a remote Windows AD server using LDAP.
While testing authentication using the CLI command diagnose test authserver. the administrator observed that authentication succeeded with PAP but failed when using MS- CHAFV2.
Which two solutions can the administrator implement to enable MS-CHAPv2 authentication? (Choose two.)

A. Change the FortiGate authentication method to CHAP instead of MS-CHAPv2.
B. Enable Windows Active Directory domain authentication on FortiAuthenticator.
C. Enable RADIUS attribute filtering on FortiAuthenticator.
D. Configure FortiAuthenticator to use RADIUS instead of LDAP as the back-end authentication server

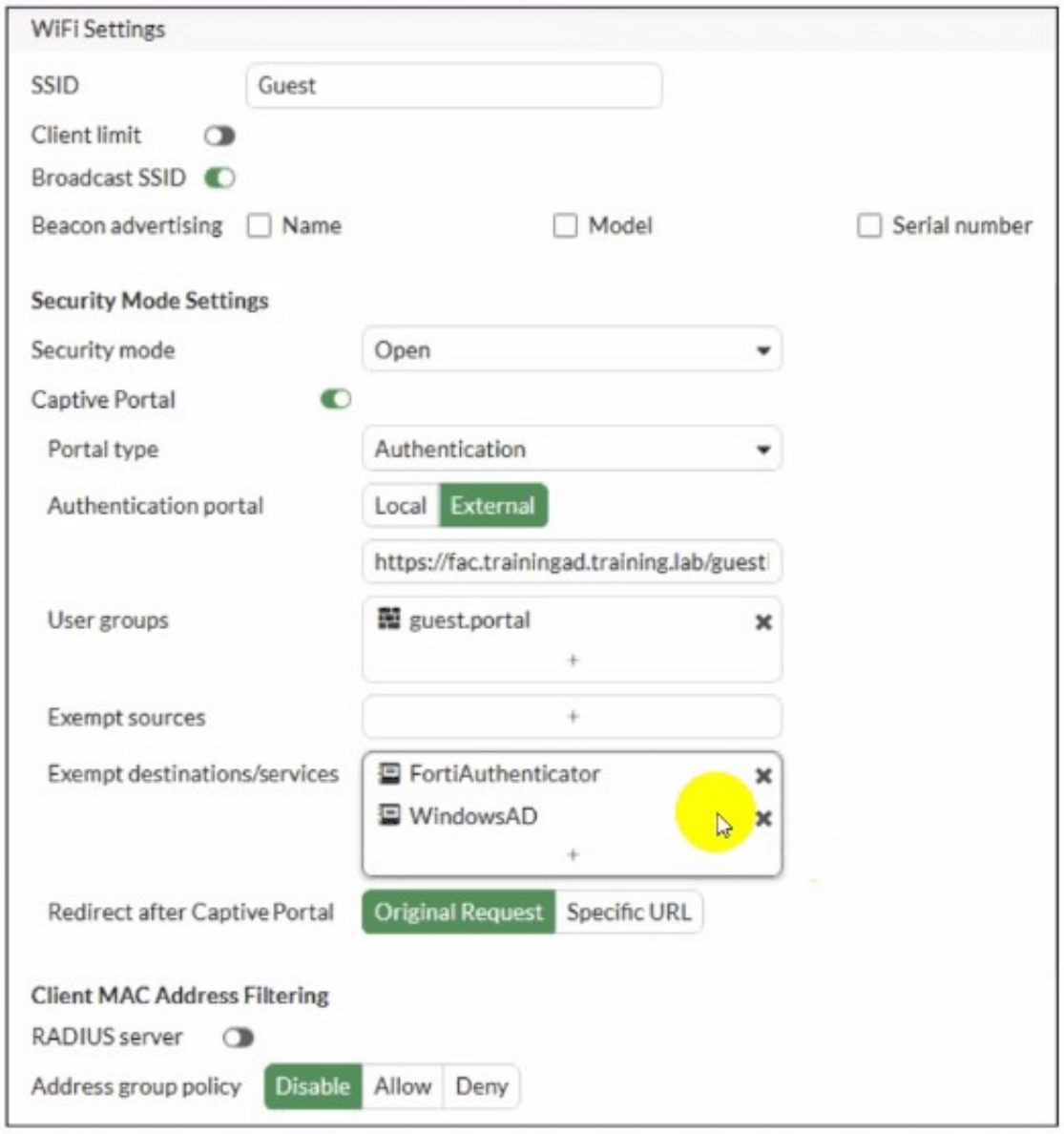
Answer: AD

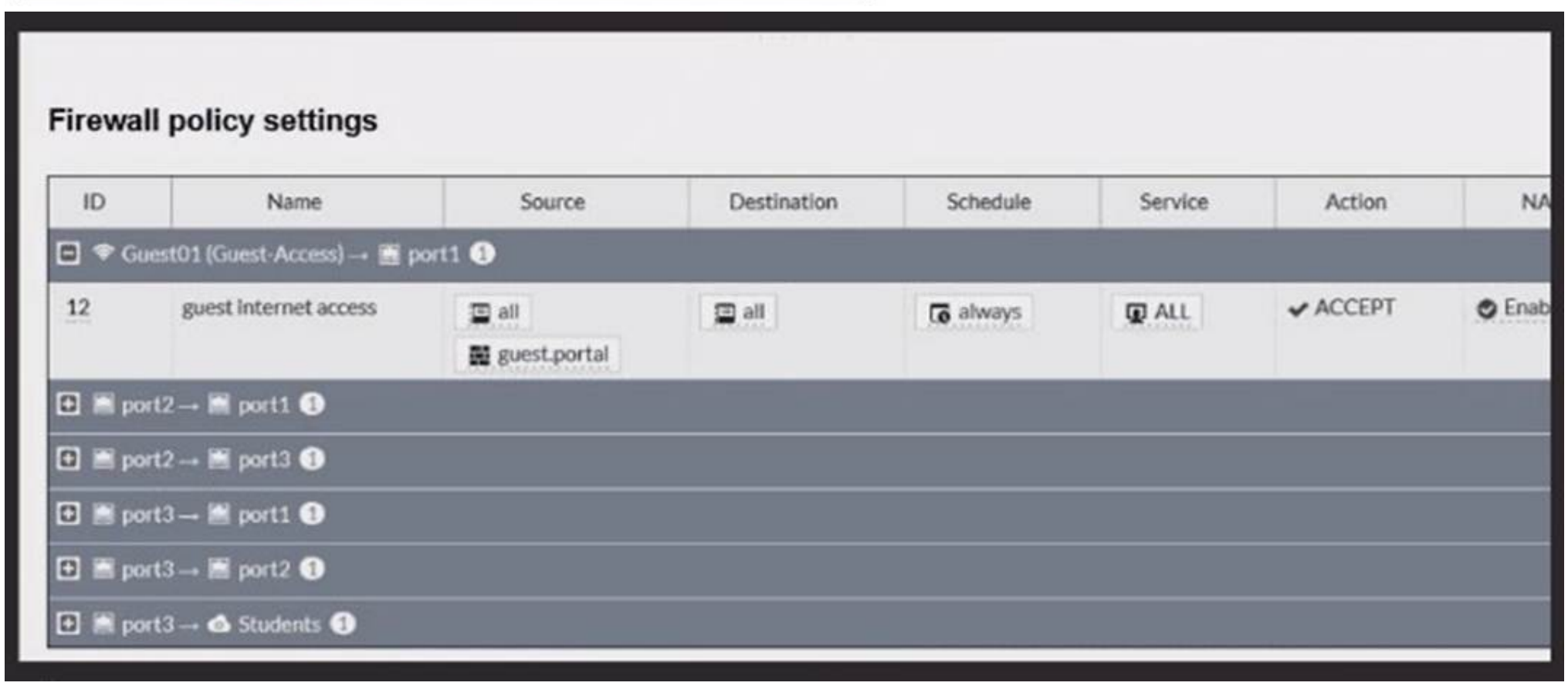
NEW QUESTION 3
Refer to the exhibit.

Network Topology



WiFi settings





Review the exhibits to analyze the network topology, SSID settings, and firewall policies.

FortiGate is configured to use an external captive portal for authentication to grant access to a wireless network. During testing, it was found that users attempting to connect to the SSID cannot access the captive portal login page.
What configuration change should be made to resolve this issue to allow users to access the captive portal?

A. Change the SSID security mode to WPA2-Enterprise for authentication.
B. Disable HTTPS redirection for the captive portal authentication page.
C. Exclude FortiAuthenticator and Windows AD address objects from filtering.
D. A firewall policy allowing Guest SSID traffic to reach FortiAuthenticator and Windows AD.

Answer: D

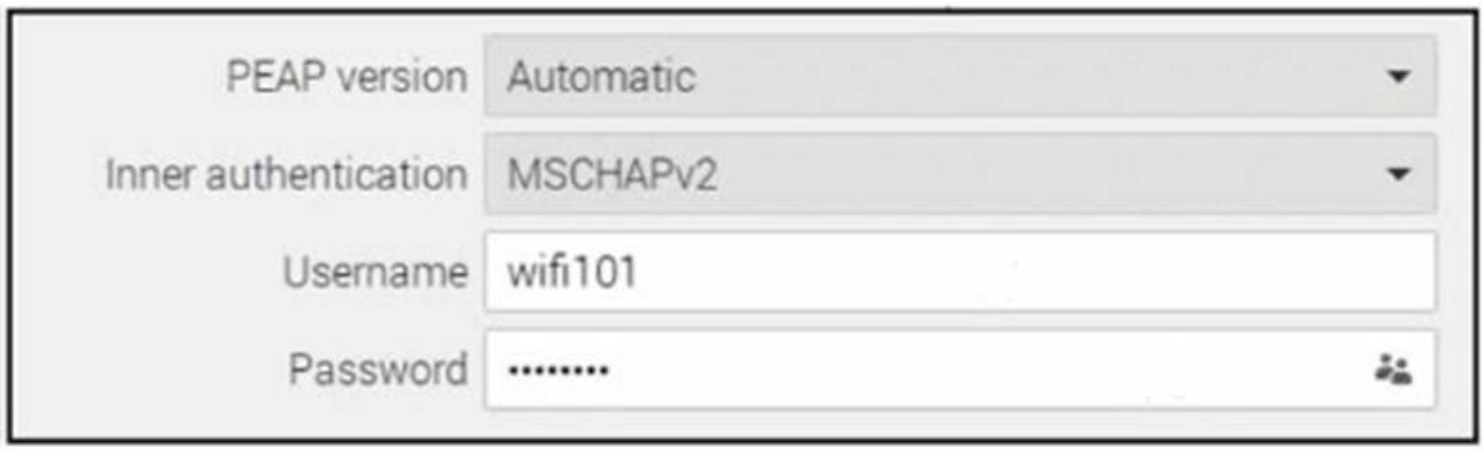
NEW QUESTION 4
Refer to the exhibits.

FortiGate LDAP server configuration and diagnostics

```
config user ldap
    edit "FAC-LDAP"
        set server "10.0.1.10"
        set cnid "sAMAccountName"
        set dn "DC=trainingAD,DC=training,DC=lab"
        set type regular
        set username "CN=Administrator,CN=Users,DC=trainingAD,DC=training,DC=lab"
        set password ENC MTAwNE2iciyoaiRa20HnjmgtQbCRYdI+OJtfO7y9+uW5V8ZxQ/Vj+mW4zPijgtCgrnAA
    next
end

FortiGate # diagnose test authserver ldap FAC-LDAP wifi101 password
authenticate 'wifi101' against 'FAC-LDAP' succeeded!
Group membership(s) - CN=Domain Users,CN=Users,DC=trainingad,DC=training,DC=lab
Domain of user is trainingad.training.lab
```

Wi-Fi Authentication

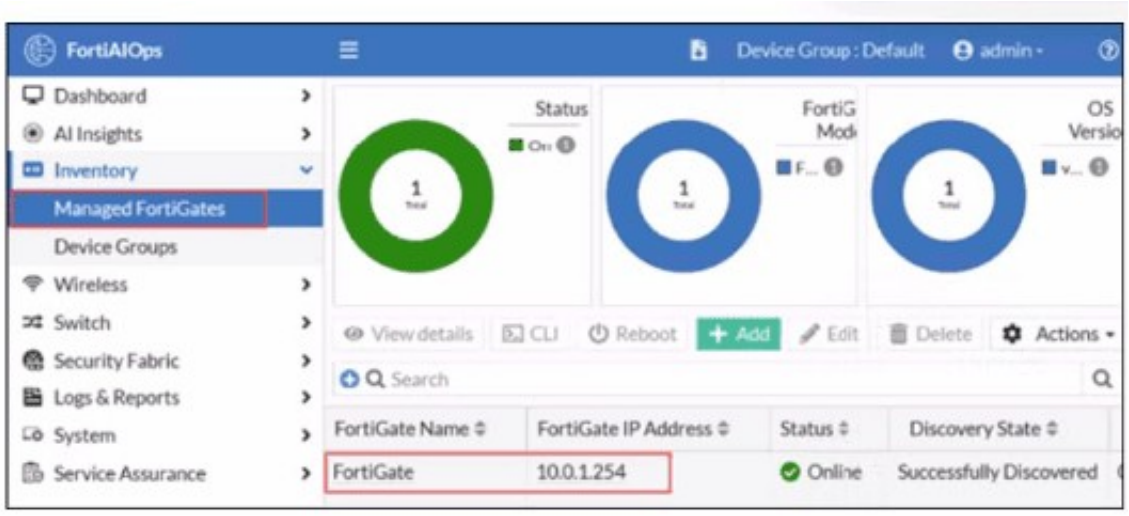


An LDAP server has been successfully configured on FortiGate. which forwards LDAP authentication requests to a Windows Active Directory (AD) server. Wireless users report that they are unable to authenticate. Upon troubleshooting, you find that authentication fails when using MSCHAPv2.
What is the most likely reason for this issue?

A. A firewall policy is missing an LDAP authentication rule.
B. The Windows AD server requires LDAPS (LDAP over SSL) for authentication.
C. The FortiGate LDAP configuration is missing the correct Bind DN.
D. FortiGate does not support MSCHAPv2 for LDAP authentication.

Answer: D

NEW QUESTION 5
FortiGate has been added to FortiAIOps for management.



Which step must be performed on FortiAIOps to add a FortiSwitch device connected to the recently added FortiGate?

A. Add the FortiSwitch device by submitting its serial number.
B. FortiAIOps requires that the FortiSwitch IP address is submitted.
C. FortiSwitch is added automatically.
D. Configure the FortiSwitch IP address, user ID, and password

Answer: C

NEW QUESTION 6
Refer to the exhibits.

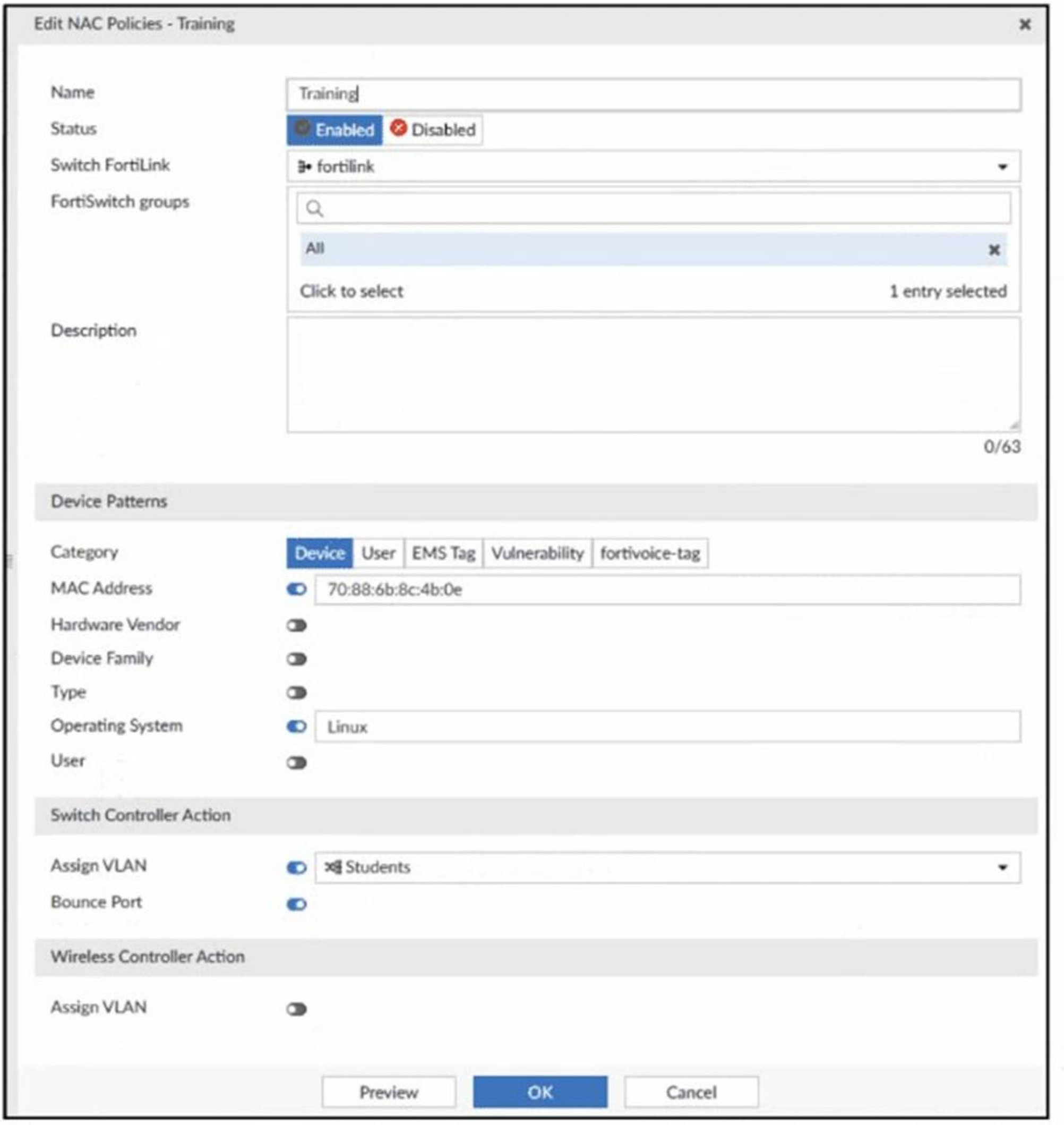
FortiSwitch Ports

FortiSwitch Ports - FortiSwitch

+ Create New | Edit | Delete | Refresh

Port	Description	Mode	Port Policy	Enabled Features	Native VLAN	Allowed VLANs
port1		Static		Edge Port Spanning Tree Protocol	AP Management (APs)	HR (VLAN102) IT (VLAN101) quarantine.fortilink (quarantine)
port2		Static		Edge Port Spanning Tree Protocol	Students	quarantine.fortilink (quarantine)
port3		Static		Edge Port Spanning Tree Protocol	default.fortilink (_default)	quarantine.fortilink (quarantine)

NAC policy



A NAC policy has been configured to apply traffic that flows through FortiSwitch port 2. Traffic that meets the NAC policy criteria will be assigned to the Students VLAN. However, the NAC policy does not seem to be taking effect.
Which configuration is missing?

A. Port2 Access mode should be set to NAC mode.
B. The MAC address or OS might be misconfigured for the connected device.
C. Port2 Access mode should be set to Port Policy mode.
D. The Students VLAN should be set to Allowed VLANs instead of Native VLAN.

Answer: A

NEW QUESTION 7
Refer to the exhibits.

FortiGate VLAN AP settings

```
config system interface
    edit "APs"
        set vdom "root"
        set ip 10.10.100.254 255.255.255.0
        set allowaccess ping
        set alias "AP Management"
        set device-identification enable
        set role lan
        set snmp-index 118
        set ip-managed-by-fortiipam disable
        set interface "fortilink"
        set vlanid 100
    next
end
```

DHCP configuration

```
config system dhcp server
    edit 7
        set dns-service default
        set default-gateway 10.10.100.254
        set netmask 255.255.255.0
        set interface "APs"
        config ip-range
            edit 1
                set start-ip 10.10.100.1
                set end-ip 10.10.100.253
            next
        end
    next
end
```

FortiSwitch port1 VLAN AP assignment

```
config switch-controller managed-switch
    edit "FortiSwitch"
        set sn "S224EPTF19006016"
        set fsw-wan1-peer "fortilink"
        set fsw-wan1-admin enable
        set poe-detection-type 2
        set version 1
        set max-allowed-trunk-members 8
        set pre-provisioned 1
        set dynamic-capability 0x00000000000000001551027757ddfff7
        config ports
            edit "port1"
                set poe-capable 1
                set vlan "APs"
                set allowed-vlans "VLAN102" "VLAN101" "quarantine"
                set untagged-vlans "quarantine"
                set export-to "root"
                set mac-addr 04:d5:90:39:7d:8e
            next
```

A FortiSwitch is successfully managed by a FortiGate. FortiAP is connected to port1 of the managed FortiSwitch. On FortiGate, the VLAN AP is configured to detect and manage FortiAP, along with a DHCP server for the VLAN AP. Additionally, the VLAN AP is assigned to port1 of FortiSwitch. However. FortiGate is unable to detect or manage FortiAP.
Which FortiGate misconfiguration is preventing the detection of FortiAP?

A. Security Fabric is disabled in the administrative access options of the VLAN.
B. The FortiAP firmware is incompatible with the FortiGate firmware version.
C. The VLAN is not tagged correctly on the FortiSwitch uplink port.
D. The CAPWAP ports (UDP 5246 and 5247) are not open on FortiGate.

Answer: A

NEW QUESTION 8
Which VLAN is used by FortiGate to place devices that fail to match any configured NAC policies? CRSPAN

A. NAC
B. segment
C. Quarantine
D. Onboarding

Answer: D

NEW QUESTION 9
In a Windows environment using AD machine authentication, how does FortiAuthenticator ensure that a previously authenticated device is maintaining its network access once the device resumes operating after sleep or hibernation?

A. It temporarily assigns the device to a guest VLAN until full reauthentication is completed.
B. It sends a wake-on-LAN packet to trigger reauthentication.
C. It uses machine authentication based on the device IP address.
D. It caches the MAC address of authenticated devices for a configurable period of time.

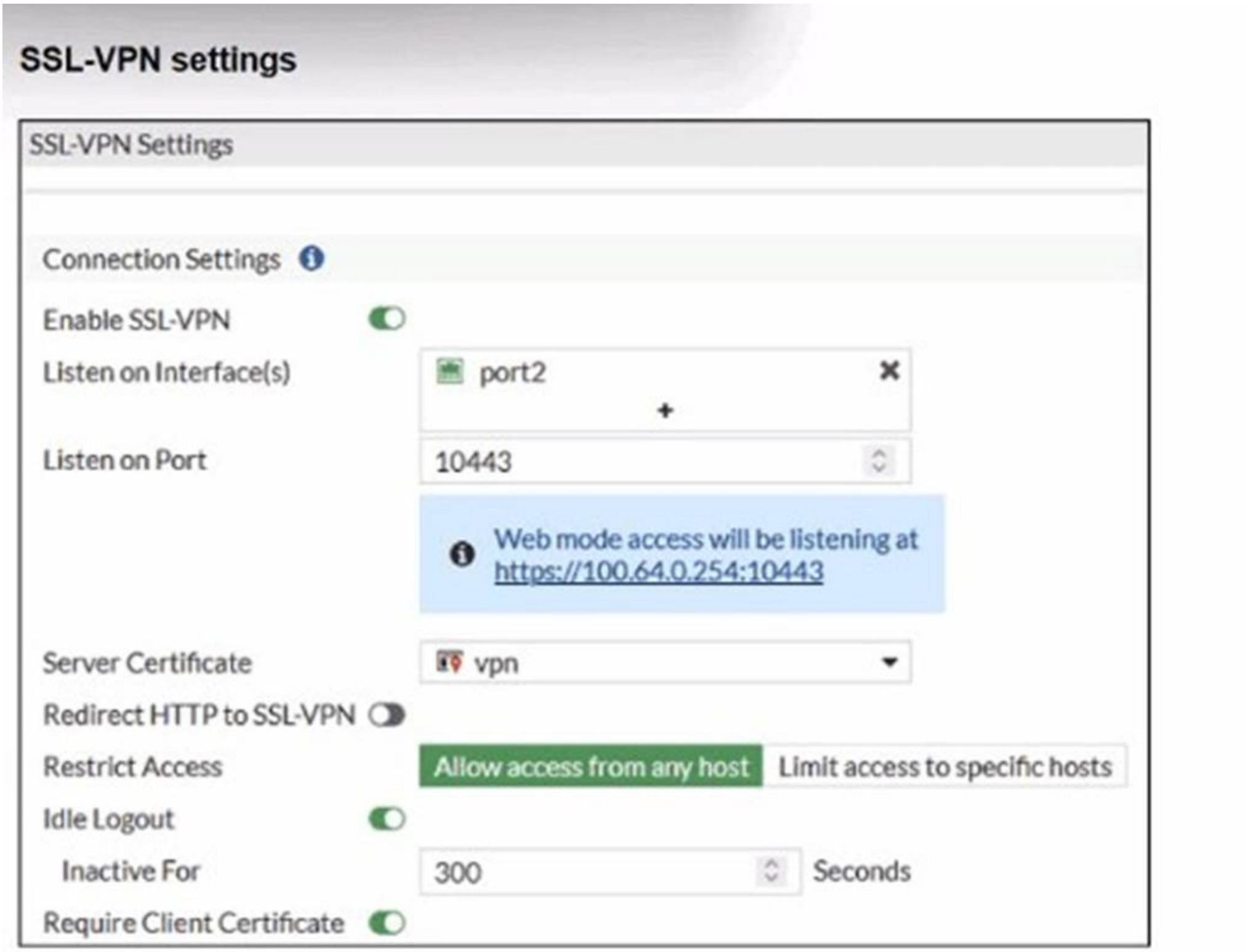
Answer: D

NEW QUESTION 10
Connectivity tests are being performed on a newly configured VLAN. The VLAN is configured on a FortiSwitch device that is managed by FortiGate. During testing, it is observed that devices within the VLAN can successfully ping FortiGate. and FortiGate can also ping these devices.
Inter-VLAN communication is working as expected. However, devices within the same VLAN are unable to communicate with each other.
What could be causing this issue?

A. Access VLAN is enabled on the VLAN.
B. The FortiSwitch MAC address table is missing entries.
C. The FortiGate ARP table is missing entries.
D. The native VLAN configured on the ports is incorrect.

Answer: A

NEW QUESTION 10
Refer to the exhibits.


SSL-VPN settings
SSL-VPN Settings
Connection Settings
Enable SSL-VPN
Listen on Interface(s)
port2
Listen on Port
10443
Web mode access will be listening at
https://100.64.0.254:10443
Server Certificate
vpn
Redirect HTTP to SSL-VPN
Restrict Access
Allow access from any host
Limit access to specific hosts
Idle Logout
Inactive For
300
Seconds
Require Client Certificate

Real-Time debug output

```
FortiGate # diagnose debug application fnbamd -1
Debug messages will be on for 30 minutes.

FortiGate # diagnose debug enable

FortiGate # [2341] handle_req-Rcvd auth_cert req id=1288058918, len=1104, opt=0
[948] __cert_auth_ctx_init-req_id=1288058918, opt=0
[103] __cert_chg_st- 'Init'
[140] fnbamd_cert_load_certs_from_req-1 cert(s) in req.
[99] __cert_chg_st- 'Init' -> 'Chain-Build'
[683] __cert_build_chain-req_id=1288058918
[200] fnbamd_chain_build-Chain discovery, opt 0x17, cur total 1
[216] fnbamd_chain_build-Following depth 0
[271] fnbamd_chain_build-Extend chain by system trust store. (no luck)
[283] fnbamd_chain_build-Extend chain by remote CA cache. (no luck)
[99] __cert_chg_st- 'Chain-Build' -> 'CA-Query'
[777] __cert_ca_query-req_id=1288058918
[769] fnbamd_need_CA_query-Do CA query?0
[793] __cert_ca_query_do_next-req_id=1288058918
[99] __cert_chg_st- 'CA-Query' -> 'Validation'
[804] __cert_verify-req_id=1288058918
[805] __cert_verify-Chain is not complete.
[200] fnbamd_chain_build-Chain discovery, opt 0x7, cur total 1
[216] fnbamd_chain_build-Following depth 0
[271] fnbamd_chain_build-Extend chain by system trust store. (no luck)
[283] fnbamd chain build-Extend chain by remote CA cache. (no luck)
```

Real-Time debug output

```
[396] fnbamd_cert_verify-Chain number:1
[410] fnbamd_cert_verify-Following cert chain depth 0
[676] fnbamd_cert_check_group_list-checking group with name 'SSLVPN'
[490] __check_add_peer-check 'student'
[460] __quick_check_peer-CA does not match.
[498] __check_add_peer-'student' check ret:bad
[193] __get_default_ocsp_ctx-def_ocsp_ctx=(nil), no_ocsp_query=0, ocsp_enabled=0
[841] __cert_verify_do_next-req_id=1288058918
[99] __cert_chg_st- 'Validation' -> 'Done'
[886] __cert_done-req_id=1288058918
[1652] fnbamd_auth_session_done-Session done, id=1288058918
[931] __fnbamd_cert_auth_run-Exit, req_id=1288058918
[1689] create_auth_cert_session-fnbamd_cert_auth_init returns 0, id=1288058918
[1608] auth_cert_success-id=1288058918
[1031] fnbamd_cert_auth_copy_cert_status-req_id=1288058918
[833] fnbamd_cert_check_matched_groups-checking group with name 'SSLVPN'
[903] fnbamd_cert_check_matched_groups-not matched
[1070] fnbamd_cert_auth_copy_cert_status-Leaf cert status is unchecked.
[1087] fnbamd_cert_auth_copy_cert_status-Issuer of cert depth 0 is not deteced in CMDB.
[1158] fnbamd_cert_auth_copy_cert_status-Cert st 2040, req_id=1288058918
[217] fnbamd_comm_send_result-Sending result 0 (nid 672) for req 1288058918, len=2144
[1553] destroy_auth_cert_session-id=1288058918
[1004] fnbamd_cert_auth_uninit-req_id=1288058918
```

Which include debug output and SSL VPN configuration details.
An SSL VPN has been configured on FortiGate. To enhance security, the administrator enabled Required Client Certificate in the SSL VPN settings. However, when a user attempts to connect, authentication fails.
Which configuration change is needed to fix the issue and allow the user to connect?

A. Enable Redirect HTTP to SSL-VPN on the SSL VPN configuration page.

B. Import the CA that signed the SSL VPN Server Certificate to FortiGate.
C. Set the user certificate as the Server Certificate on the SSL VPN configuration page.
D. Import the CA that signed the user certificate to FortiGate.

Answer: D

NEW QUESTION 11
A conference center wireless network provides guest access through a captive portal, allowing unregistered users to self-register and connect to the network. The IT team has been tasked with updating the existing configuration to enforce captive portal authentication over a secure HTTPS connection. Which two steps should the administrator take to implement this change? (Choose two.)

A. Enable HTTP redirect in the user authentication settings.
B. Create a new SSID with the HTTPS captive portal URL.
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.

Answer: AD

NEW QUESTION 14
APs have been manually configured to connect to FortiGate over an IPsec network, and FortiGate successfully detects and authorizes them. However, the APs remain unmanaged because FortiGate is unable to establish a CAPWAP tunnel with them.
What configuration change can resolve this issue and enable FortiGate to establish the CAPWAP tunnel over the IPsec connection?

A. Configure a static route on FortiGate to reach the APs over the IPsec tunnel.
B. Assign a custom AP profile for the remote APs with the set mpls-connection option enabled.
C. Decrease the CAPWAP tunnel MTU size for APs to prevent fragmentation.
D. Upgrade the FortiAP firmware image to ensure compatibility with the FortiOS version.

Answer: B

NEW QUESTION 18
You've configured the FortiLink interface, and the DHCP server is enabled by default.

```
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
```

The resulting DHCP server settings are shown in the exhibit. What is the role of the vci-string setting in this configuration?

A. To ignore DHCP requests coming from FortiSwitch and FortiExtender devices.
B. To restrict the IP address assignment to devices that have FortiSwitch or FortiExtender as their hostname.
C. To connect, devices must match the VCI string; otherwise, they will not receive an IP address.
D. To reserve IP addresses for FortiSwitch and FortiExtender devices.

Answer: C

NEW QUESTION 23
In each user certificate, you can define the subject field, expiration date. User Principal Name (UPN), URL for CRL download, and the OCSP URL. How does the detailed configuration of these attributes impact the certificate?

A. It makes the certificate easier to revoke manually because it reduces the need for automatic checks.

B. It limits the validity of the certificate to specific devices and applications, reducing its general usability.
C. It enables precise identification of the user and ensures timely certificate revocation checks.
D. It makes the certificate compatible with a wide range of applications and services by ensuring universal validity

Answer: C

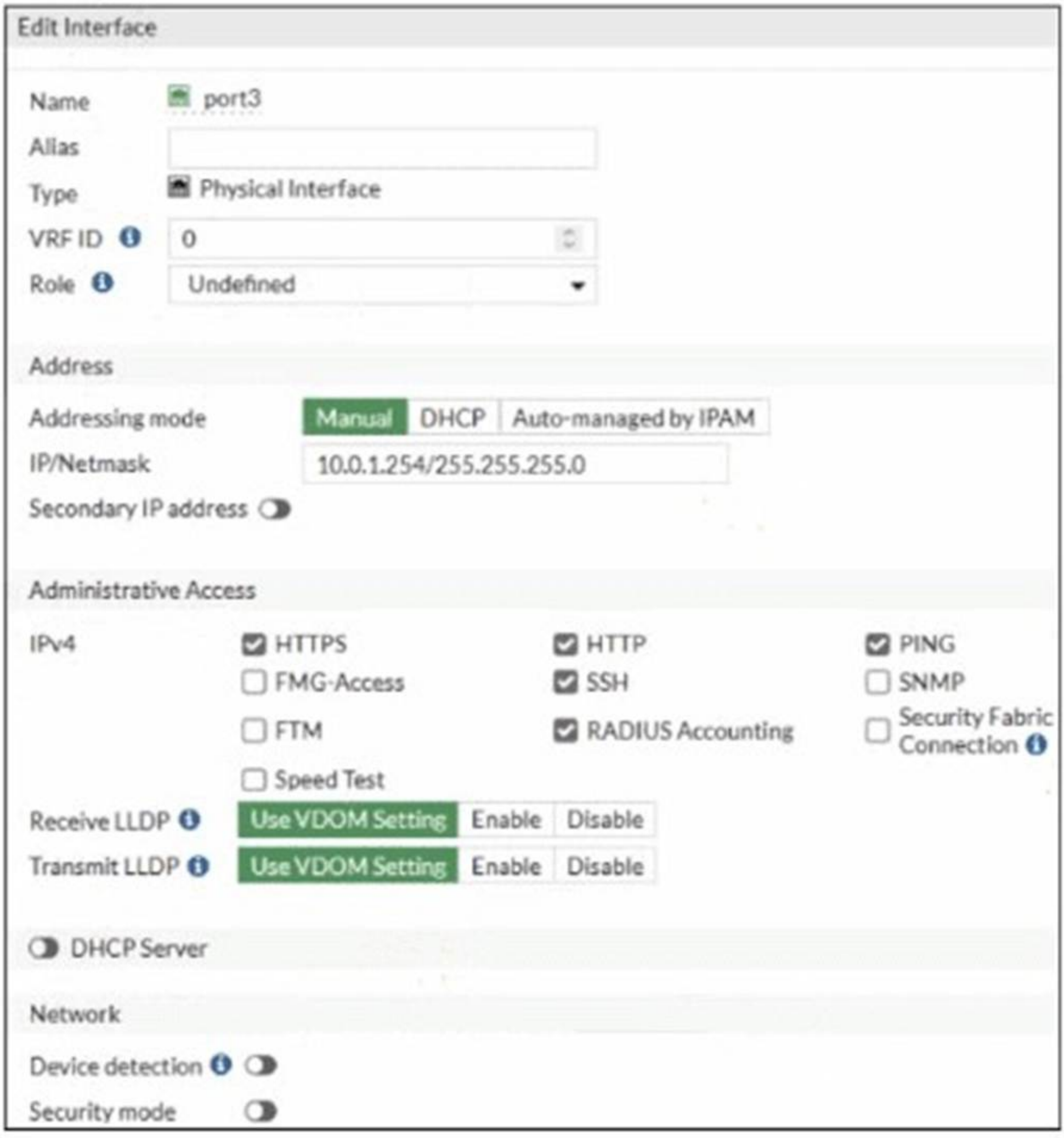
NEW QUESTION 24
When troubleshooting a captive portal issue, which POST parameter in the redirected HTTPS request can be used to track the user's session and ensure that the request is valid?

A. username
B. redir
C. magic
D. email

Answer: C

NEW QUESTION 29
Refer to the exhibits.

FortiGate interface configuration



Examine the FortiGate RSSO configuration shown in the exhibit.
FortiGate is set up to use RSSO for user authentication. It is currently receiving RADIUS accounting messages through port3. The incoming RADIUS accounting messages contain the username in the User-Name attribute and group membership in the Class attribute. You must ensure that the users are authenticated through these RADIUS accounting messages and accurately mapped to their respective RSSO user groups.
Which three critical configurations must you implement on the FortiGate device? (Choose three.)

A. The RADIUS Attribute Value setting configured for an RSSO user group should match the class RADIUS attribute value in the RADIUS accounting message.
B. RSSO user groups should be assigned to all firewall policies.
C. Device detection and Security Fabric Connection should be enabled on port3
D. The sso-attribute CLI setting in the RSSO agent configuration should be set to Class.
E. The rsso-endpoint-attribute CLI setting in the RSSO agent configuration should be set toUser-Name.

Answer: ADE

NEW QUESTION 33

.....

Relate Links

100% Pass Your FCSS_LED_AR-7.6 Exam with Exambible Prep Materials

https://www.exambible.com/FCSS_LED_AR-7.6-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/