Fortinet
FCSS_LED_AR-7.6
Fortinet FCSS - LAN Edge 7.6 Architect

For More Information – Visit link below:
https://www.examsempire.com/

Product Version

1. Up to Date products, reliable and verified.
2. Questions and Answers in PDF Format.

Latest Version: 8.0

Question: 1

In addition to requiring a FortiAnalyzer device to configure the Security Fabric, which license must be added to FortiAnalyzer to use Indicators of Compromise (IOC) rules?

A. loT Security Add-on license
B. IOC Subscription license
C. IOC detection is included on FAZ-Basic license
D. Threat Detection Service license

Answer: D

Explanation:
FortiAnalyzer requires a specific license to evaluateIndicators of Compromise (IOC).
From theFortiAnalyzer 7.4.1 Administration Guide:
IOC identification requires theThreat Detection Servicelicense on FortiAnalyzer.
This license enables:
IOC database updates
Compromised host detection
Event correlation based on FortiGuard threat intelligence
Fabric-wide IOC automation triggers
Why the other answers are incorrect:
A: IoT Security add-on is unrelated to IOC rules.
B: There isnoIOC subscription license type for FortiAnalyzer.
C: FAZ-Basic license doesNOTinclude IOC detection.

Question: 2

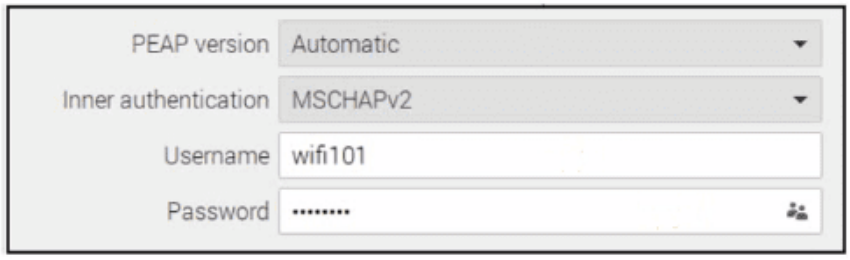
Refer to the exhibits.

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.

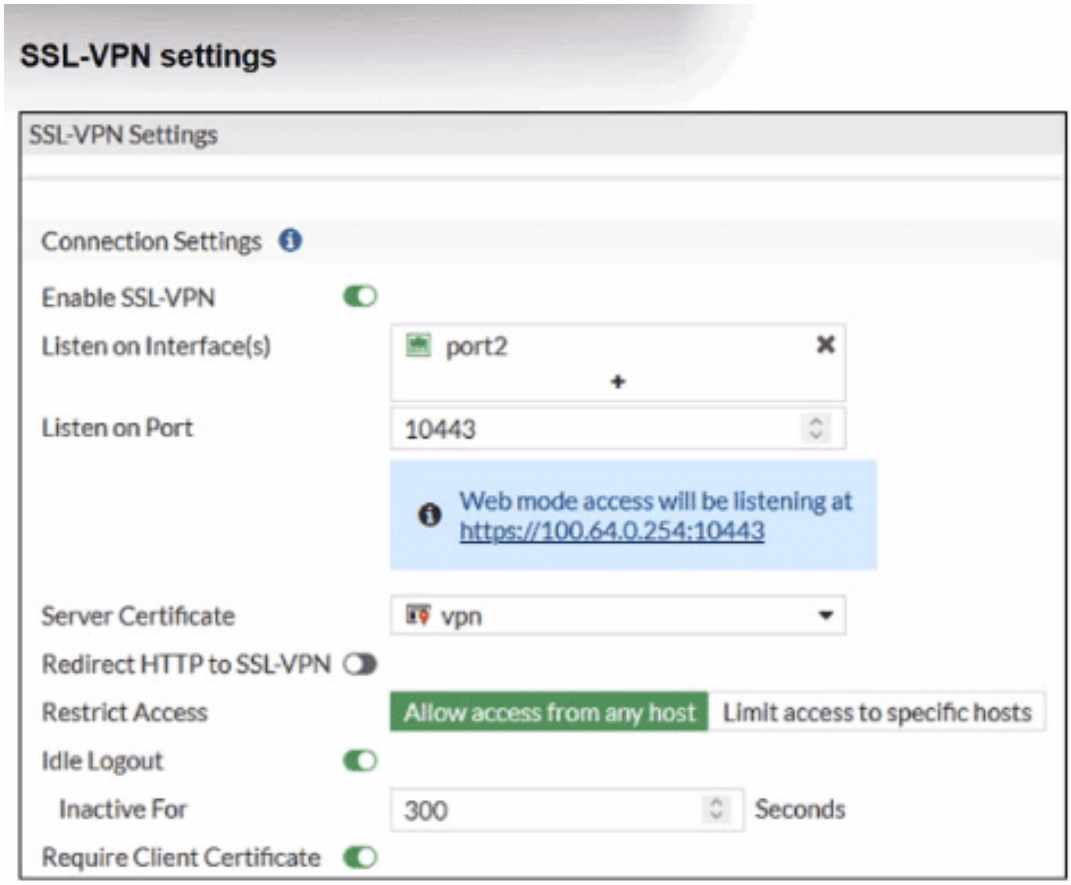
Answer: D

Explanation:
From the exhibit, LDAP on FortiGate is correctly configured and tested:
diagnose test authserver ldap FAC-LDAP wifi101 password
authenticate 'wifi101' against 'FAC-LDAP' succeeded!
Group membership(s) - CN=Domain Users,...
So:
LDAP connectivity works

Bind DN, DN, CNID, and credentials are correct(so optionCis eliminated).
Firewall policies do not affect the802.1X / Wi-Fi authentication stepitself, soAis not the root cause.
Nothing in the scenario indicates that AD is enforcing LDAPS-only; the LDAP test already succeeds using the configured parameters, soBis also excluded.
The Wi-Fi supplicant is configured forPEAP with inner authentication = MSCHAPv2.
MSCHAPv2 is achallenge–response mechanism designed for RADIUS, not for LDAP simple bind.
FortiGate's LDAP implementation uses asimple bind (username/password) over LDAP or LDAPS, and it doesnotimplement MSCHAPv2 against LDAP backends.
In Fortinet's design, if you needPEAP-MSCHAPv2 with Active Directory, you must use:
ARADIUS server(such as Windows NPS or FortiAuthenticator), and
Have FortiGate use RADIUS,notLDAP, as the authentication backend for 802.1X / Wi-Fi users.
Because FortiGate cannot process MSCHAPv2 exchanges directly against an LDAP server, authentication fails when the inner method is MSCHAPv2, even though LDAP works when tested with a simple bind from the CLI.

Question: 3

Refer to the exhibits.



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.

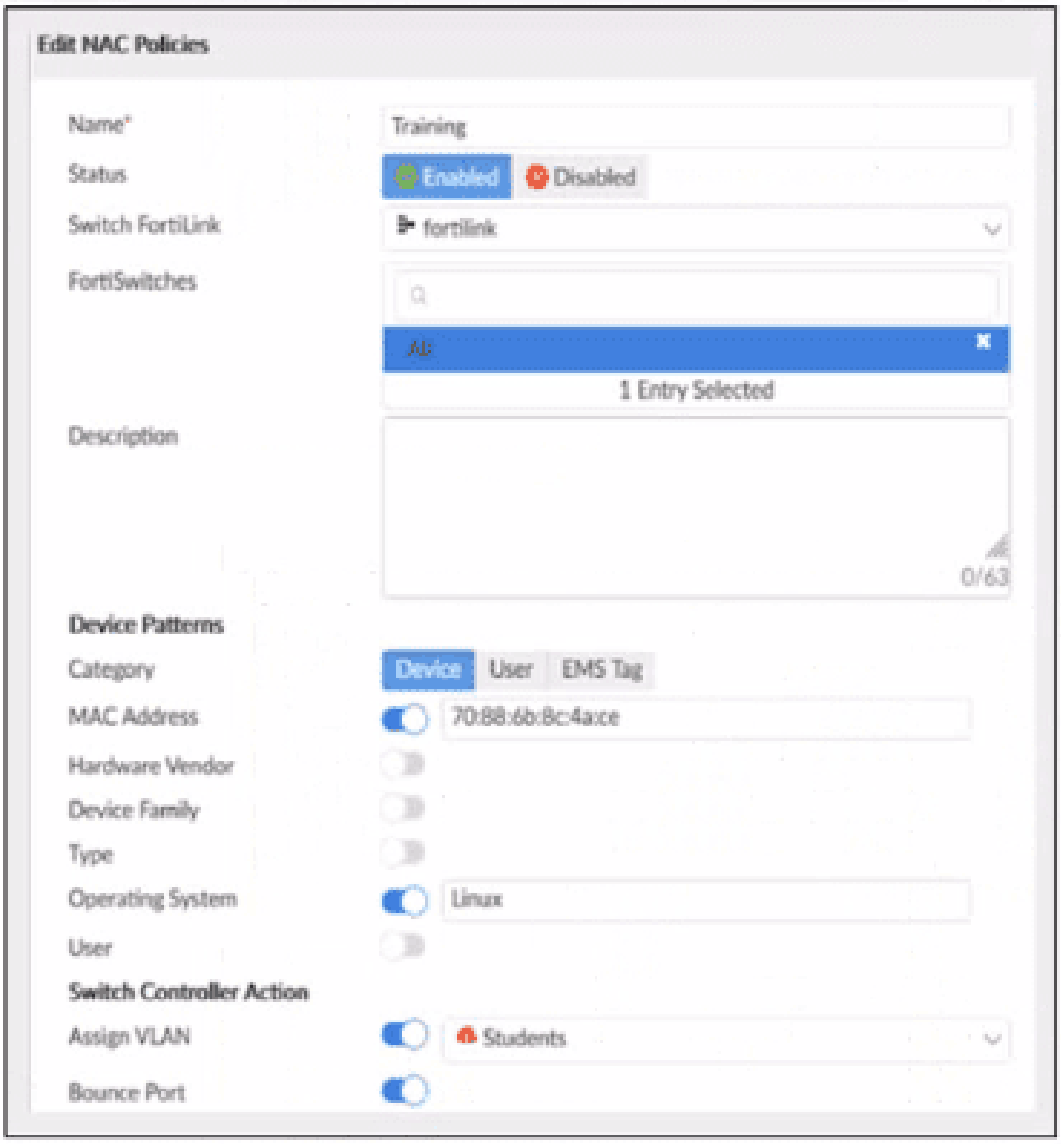
Answer: D

Explanation:
The SSL-VPN configuration hasRequire Client Certificateenabled. When this is enabled, FortiOS performs two checks:
Normal user authentication(username/password or PKI user)
Additional client certificate check– the client certificatemust be signed by a CA that FortiGate trusts
FortiOS documentation for “SSL VPN with certificate authentication” states:
“The client certificate only needs to be signed by a known CA in order to pass authentication.”
“The CA certificate is the certificate that signed both the server certificate and the user certificate… The CA certificate is available to be imported on the FortiGate.”
The debug output shows key lines:
__quick_check_peer-CA does not match.
Issuer of cert depth 0 is not detected in CMDB.
This tells us:
FortiGatedoes see the user’s certificate,
Butcannot find the issuing CAin its local CA certificate store (“CMDB” = configuration database).
This means theCA that signed the user certificate has not been importedinto FortiGate.
Now evaluate the options:
A . Enable Redirect HTTP to SSL-VPN– affects only redirection from HTTP to HTTPS; it has nothing to do with certificate validation.
B . Import the CA that signed the SSL VPN Server Certificate– the server certificate is already working (the portal comes up) and its CA is not what the debug complains about; the error is about thepeer (user) certificate. Often the same CA signs both, but the failing check specifically says the issuer of the client cert is not in CMDB.
C . Set the user certificate as the Server Certificate– incorrect; server and client certificates serve different roles.
D . Import the CA that signed the user certificate to FortiGate– this directly addresses the debug error and aligns with the documented requirement that the CA which issued the user certificate must be known to FortiGate.

Question: 4

Refer to the exhibits.

FortiManager configuration



FortiGate CLI output

```
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 I

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:29:06: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   FSW-ID  COMMENTS
```

Examine the FortiManager configuration and FortiGate CLI output shown in the exhibit.
The NAC feature is being tested with a device connected to port2 on managed FortiSwitch S224SPTF19005867. The NAC policy has been applied to port2, and traffic was generated from the test device. However, the traffic from the test device does not match the NAC policy and remains in the onboarding VLAN.
What are two possible reasons why the test device is not being correctly classified by the NAC policy? (Choose two.)

A. Device detection is not enabled on VLAN 4089.
B. The device operating system detected by FortiGate is not Linux.
C. Management communication between FortiGate and FortiSwitch is down.
D. The MAC address configured on the NAC policy is incorrect.

Answer: A, B

Explanation:
From the FortiManager NAC policy:
Category =Device
Match criteria includeMAC addressandOperating System = Linux
Action =Assign VLAN “Students”
From the FortiGate CLI:
diagnose switch-controller switch-info mac-table ...
MAC: 70:88:6b:8c:4a:ce VLAN: 4089 Port: port2
diagnose switch-controller mac-device mac onboarding

VLAN 4089 MAC 70:88:6b:8c:4a:ce
So the device is stuck inVLAN 4089, which is theonboarding VLAN. No NAC policy is matched.
For a NAC policy to match, FortiGate needsdevice-identity information, which comes fromdevice detection on the VLAN / FortiLink interfaceplus theattributes that the policy expects(OS, MAC, etc.).
A . Device detection is not enabled on VLAN 4089.
If device detection is disabled on the interface/VLAN where the endpoint lives, FortiGate cannot learn OS / device info.
Without this, the NAC engine cannot compare against the NAC policy (which relies on OS and other attributes), so the device remains in the onboarding VLAN.This is a valid root cause.
B . The device operating system detected by FortiGate is not Linux.
The NAC policy explicitly requiresOperating System = Linux.
If the endpoint is actually Windows/macOS, or the OS fingerprint is still “Unknown”, the policy will never match, and the device stays in onboarding.Also a valid reason.
C . Management communication between FortiGate and FortiSwitch is down.
CLI output (switch-info mac-table and mac-device) proves FortiGate is talking to the switch and sees MAC/VLAN/port information.Not a valid reason.
D . The MAC address configured on the NAC policy is incorrect.
The exhibits show the MAC in the NAC policy matches the MAC appearing in the MAC table.Not the cause here.

Question: 5

A FortiSwitch is not appearing in the FortiGate management interface after being connected via FortiLink. What could be a first troubleshooting step?

A. Ensure that the FortiGate security policies allow traffic from the FortiSwitch.
B. Manually assign a static IP to the FortiSwitch.
C. Verify that FortiGate device DHCP server is assigning an IP to the FortiSwitch.
D. Ensure the FortiSwitch has internet access.

Answer: C

Explanation:
In FortiLink topologies, a managed FortiSwitch normally gets itsmanagement IP automaticallyfrom theDHCP server on the FortiLink interface. If the switch does not receive an IP:
It cannot form the FortiLink CAPWAP/DTLS control channel.
Therefore it doesnot appearunderWiFi & Switch Controller > FortiSwitch.
FortiOS documentation states that FortiLink uses abuilt-in DHCP serveron the FortiLink interface for onboarding switches.
So thefirst troubleshooting stepis to confirm:
The FortiLink DHCP server is enabled.
Leases are being handed out to the FortiSwitch MAC.
Other options:

A: Security policies do not affect the L2 FortiLink control channel.
B: Static IP may be used but is not the normal first step.
D: Internet access is not required for FortiGate to see the switch.

Thank You for Trying Our Product

Special 16 USD Discount Coupon: NSZUBG3X

Email: support@examsempire.com

Check our Customer Testimonials and ratings available on every product page.

Visit our website.

https://examsempire.com/