

Fortinet

Exam Questions FCSS_LED_AR-7.6

FCSS - LAN Edge 7.6 Architect



NEW QUESTION 1

You are configuring FortiAuthenticator to integrate with FSSO for user identification. To enable FortiAuthenticator to extract user information from syslog messages and inject it into FSSO, you have configured syslog matching rules.

What is the role of syslog matching rules in the process of injecting user information into FSSO?

- A. To automatically update user group memberships in FSSO based on syslog events
- B. To enforce user authentication policies based on syslog message contents
- C. To define how syslog messages are parsed and extract user information, such as usernames and IP addresses
- D. To filter and block irrelevant syslog messages from being processed by the FortiAuthenticator

Answer: C

NEW QUESTION 2

Refer to the exhibit.

WTP profile configuration

```
config wireless-controller wtp-profile
  edit "S231F"
    config platform
      set type 231F
    end
    set handoff-rssi 30
    set handoff-sta-thresh 30
    set ap-country US
    config radio-1
      set band 802.11n-2G
      set wids-profile "default-wids-apscan-enabled"
      set vap-all manual
      set vaps "Student01"
      set channel "1" "6" "11"
    end
    config radio-2
      set band 802.11ac-5G
      set channel-bonding 40MHz
      set wids-profile "default-wids-apscan-enabled"
      set darrp enable
      set arrp-profile "arrp-default"
      set vap-all manual
      set vaps "Student01"
      set channel "36" "44" "52"
    end
    config radio-3
      set mode disabled
    end
  next
end
```

Which shows the WTP profile configuration.

The AP profile is assigned to two FAP-231F APs that are installed in an open plan area. The first AP has 32 clients associated with the 5 GHz radios and 22 clients associated with the 2.4 GHz radio. The second AP has 12 clients associated with the 5 GHz radios and 20 clients associated with the 2.4 GHz radio.

A dual-band-capable client enters the area 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.

If the new client attempts to connect to the student 01 wireless network, which AP radio will the client be associated with?

- A. The first AP 2.4 GHz interface provides a stronger signal, which clients often prioritize.
- B. The first AP 5 GHz interface because it has a stronger signal.
- C. The second AP 5 GHz interface has fewer clients, which ensures better performance despite the weaker signal.
- D. The second AP 2.4 GHz interface is preferred over 5 GHz for better speed and lower interference.

Answer: C

NEW QUESTION 3

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+OJtf07y9+uW5V8ZxQ/Vj+mW4zPijgtCgrnAA
  next
end

FortiGate # diagnose test authserver ldap FAC-LDAP wifil01 password
authenticate 'wifil01' 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

PEAP version	Automatic
Inner authentication	MSCHAPv2
Username	wifi101
Password	

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 4

A network engineer is deploying FortiGate devices using zero-touch provisioning (ZTP). The devices must automatically connect to FortiManager and receive their configurations upon first boot. However, after powering on the devices, they fail to register with FortiManager. What could be a possible cause of this issue?

- A. The FortiGate device requires manual intervention to accept the FortiManager connection.
- B. In this scenario, the ZTP process works only when devices are connected using a console cable.
- C. The FortiGate device must be preloaded with a configuration file before ZTP can function.
- D. The FortiManager IP address is not reachable over TCP port 541.

Answer: D

NEW QUESTION 5

Which statement about generating a certificate signing request (CSR) for a CER certificate is true?

- A. Inaccurate or missing fields in the CSR will prevent the CA from validating the request, leading to the rejection of the certificate and possible delays in the deployment process.
- B. If key fields like the common name (CN) and organization (O) are incorrect, the certification authority (CA) will still issue the certificate, but it may not be trusted by certain applications or systems that rely on accurate field information for validation.
- C. CSR fields are primarily used for internal recordkeeping by the requesting organization, and only the public key in the CSR must be accurate for successful certificate signing.
- D. The fields in the CSR are primarily for documentation purposes; any missing or incorrect information will be automatically corrected by the CA during the signing process.

Answer: A

NEW QUESTION 6

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 ☒

Passing Certification Exams Made Easy

visit - <https://www.surepassexam.com>

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 detected 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 7

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 8

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 9

Refer to the exhibits.



FortiGate interface configuration

Edit Interface

Name

 port3

Alias

Type

 Physical Interface

VRF ID 

0



Role 

Undefined



Address

Addressing mode

Manual

DHCP

Auto-managed by IPAM

IP/Netmask

10.0.1.254/255.255.255.0

Secondary IP address



Administrative Access

IPv4

☒ HTTPS

☐ FMG-Access

☐ FTM

☐ Speed Test

☒ HTTP

☒ SSH

☒ RADIUS Accounting

☒ PING

☐ SNMP

☐ Security Fabric Connection 

Receive LLDP 

Use VDOM Setting

Enable

Disable

Transmit LLDP 

Use VDOM Setting

Enable

Disable

 DHCP Server

Network

Device detection 



Security mode



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 rso-endpoint-attribute CLI setting in the RSSO agent configuration should be set toUser-Name.

Answer: ADE

NEW QUESTION 10

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

FCSS_LED_AR-7.6 Practice Exam Features:

- * FCSS_LED_AR-7.6 Questions and Answers Updated Frequently
- * FCSS_LED_AR-7.6 Practice Questions Verified by Expert Senior Certified Staff
- * FCSS_LED_AR-7.6 Most Realistic Questions that Guarantee you a Pass on Your First Try
- * FCSS_LED_AR-7.6 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The FCSS_LED_AR-7.6 Practice Test Here](#)