Download Fortinet FCSS_LED_AR-7.6 Exam Dumps Free

Shared by Dotson on 17-06-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

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?

Options:

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

Explanation:

When FortiAuthenticator is used as anFSSO agentbased onsyslog, it must:

Parse incoming syslog messagesfrom devices (firewalls, WLAN controllers, VPN concentrators, etc.).

Extract identity fieldssuch as:

Username

IP address

Login/logout event indicators

Syslogmatching ruleson FortiAuthenticator define:

Which syslog messages are relevant (by facility, message pattern, or regex).

How to capture specific fields (username, IP, group, event type).

FortiAuthenticator then uses this parsed data toinject logon sessions into FSSO, so FortiGate can apply identity-based policies.

Thus, the role of syslog matching rules is exactly as described inC.

A: Group mapping is handled separately via directory groups / FSSO config, not directly by matching rules.

B: Enforcement of authentication policies is done on FortiGate, not directly by the matching rules.

D: While irrelevant logs can be ignored via rules, the primary purpose isparsing and extraction, not generic filtering.

Question 2

Question Type: MultipleChoice

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?

Options:

A- IoT 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 3

Question Type: MultipleChoice

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

Options:

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.

Question 4

Question Type: MultipleChoice

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

Options:

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

Explanation:

The FortiOS documentation explicitly states that a CSR used for certificate signing must contain accurate and valid fields, especially:

Common Name (CN)

Organization (O)

Country (C)

Public key parameters

According to the FortiGate certificate section:

Incorrect CSR field information can cause the CA to reject the request.

Reasons include:

The CA validates identity and organizational information.

Missing or malformed data invalidates PKI requirements.

The CSR is not corrected automatically by the CA.

Therefore:

A is correct.

Options B--D contradict PKI principles:

B is false: CAs do not issue certificates with mismatched identity fields for public trust.

C is false: CSR fields are not only for internal use; they define certificate identity.

D is false: CAs do not auto-correct CSR fields.

Question 5

Question Type: MultipleChoice

Refer to the exhibits.

VAP configuration

```
config wireless-controller vap
    edit "Corporate"
        set ssid "Corp"
        set security wpa2-only-enterprise
        set auth radius
        set radius-server "FAC-Lab"
        set intra-vap-privacy enable
        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
```

Wi-Fi zone table

WiFi SSID 7			
Corp (Corporate)	WiFi SSID		0.0.0.0/0.0.0.0
Corp.101	VLAN		0.0.0.0/0.0.0.0
Corp.102	VLAN		10.0.20.1/255.255.255.0
wqtn.5.Corporat	VLAN		0.0.0.0/0.0.0.0
Guest (Guest)	WiFi SSID		0.0.0.0/0.0.0.0
Student01 (Student01)	WiFi SSID		0.0.0.0/0.0.0.0
Zone 1			
Corp.zone	Zone	Corp.101 Corp.102	

The exhibits show the VAP configuration. Wi-Fi SSIDs. and zone table.

Which two statements describe how FortiGate handles VLAN assignment for wireless clients? (Select two.)

Options:

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- All clients connecting to the Corp Zone will receive an IP address from the 10.0.20.0/24 subnet.

C- Clients connecting to APs in the Floor 1 group will not be able to receive an IP address.

D- Clients connecting to APs in the Office group will be assigned to VLAN 102.

Answer:

C, D

Explanation:

The VAP configuration clearly showsVLAN pooling using WTP-groups:

set vlan-pooling wtp-group

config vlan-pool

edit 101

set wtp-group 'Floor_1'

edit 102

set wtp-group 'Office'

How VLAN assignment works in this mode

VLAN-pooling with wtp-group modemeans:

Each AP group (WTP group) is tied to exactly one VLAN in the pool.

The FortiGate doesnot load balanceVLANs.

Instead, VLANs are mappedper AP group, not per client.

Now verify each answer option:

A . FortiGate will load balance clients using VLAN 101 and 102...

Incorrect.

FortiGatedoes NOT load-balance clientswhen vlan-pooling is set towtp-group.

Each AP group receivesonly the VLAN mapped to it.

B . All clients in the Corp zone get IPs from 10.0.20.0/24

Incorrect.

In the Wi-Fi zone table, onlyCorp.102has an IP subnet:

Corp.101 0.0.0.0/0.0.0.0(no IP assigned clients get no DHCP)

Corp.102 10.0.20.1/255.255.255.0

Thus, clients associated to VLAN 101cannotget IPs.

C . Clients connecting to APs in the Floor_1 group cannot receive an IP address

Correct.

Reason:

Floor_1 WTP-group VLAN101

VLAN 101 hasno IPin the Wi-Fi table 0.0.0.0/0.0.0.0

No DHCP =Clients receive no IP address

D . Clients connecting to APs in the Office group will be assigned to VLAN 102

Correct.

Reason:

Office WTP-group maps to VLAN102

VLAN 102 has subnet10.0.20.0/24

So Office group clients get an IP in that range

Question 6

Question Type: MultipleChoice

How can FortiAIOps help optimize network performance in an SD-Branch deployment with FortiGate, FortiSwitch, and FortiAP?

Options:

A- It disables low-performing APs and switches automatically.
B- It uses Al-driven analytics to identify network issues and provide optimization recommendations.
C- It removes the need for SD-WAN configuration by automating all routing decisions.
D- It predicts and resolves all network issues without any human intervention.

Answer:

B

Explanation:

In an SD-Branch deployment (FortiGate + FortiSwitch + FortiAP),FortiAIOps:

Collects telemetry and logs from Fabric devices

Usesmachine-learning / AI analyticsto:

Spot anomalies (latency, packet loss, RF issues, misconfigurations)

Highlight root causes

Proposeoptimization recommendations(e.g., channel changes, power tuning, config fixes)

It doesnot:

Automatically disable devices (Afalse)

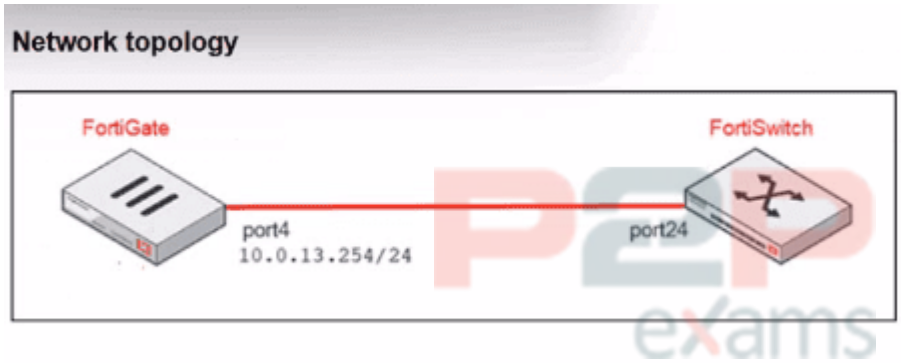
Replace SD-WAN config or all routing (Cfalse)

Fixallissues with zero human input (Dis marketing fantasy, not reality)

Question 7

Question Type: MultipleChoice

Refer to the exhibits.



FortiSwitch status

Name	Switch Group	Status	Model
FortiLink: fortilink 1			
FortiSwitch		Offline	FortiSwitch 224E-PO

Fortilink interface settings in FortiGate

```
FortiGate (fortilink) # show
config system interface
    edit "fortilink"
        set vdom "root"
        set fortilink enable
        set ip 10.0.13.254 255.255.255.0
        set allowaccess ping fabric
        set type aggregate
        set member "port4"
        set device-identification enable
        set lldp-reception enable
        set lldp-transmission enable
        set role lan
        set snmp-index 14
        set auto-auth-extension-device enable
        set ip-managed-by-fortiipam disable
        set switch-controller-nac "fortilink"
        set switch-controller-dynamic "fortilink"
        set swc-first-create 255
        set lacp-mode static
    next
end
```

DHCP server setting for fortilink

```
config system dhcp server
    edit 1
        set dns-service default
        set ntp-service local
        set default-gateway 10.0.13.254
        set netmask 255.255.255.0
        set interface "fortilink"
        config ip-range
            edit 1
                set start-ip 10.0.13.1
                set end-ip 10.0.13.253
            next
        end
        set vci-match enable
        set vci-string "FortiExtender"
    next
end
```

You are adding a new FortiSwitch to FortiGate for management. All necessary settings have been configured on FortiGate, but FortiSwitch remains offline. The cabling has been verified and is correctly connected.

Which misconfiguration might be preventing FortiGate from detecting FortiSwitch?

Options:

A- The Fortilink interface setting ip-managed-by-fortiipam must be enabled.
B- The Fortilink interface has the wrong interface member.
C- The Fortilink interface setting cype must be physical.
D- The DHCP server setting vci-string is misconfigured.

Answer:

D

Explanation:

On FortiLink, FortiGate's built-in DHCP server is what gives FortiSwitch its IP so it can come under management. For automatic FortiSwitch onboarding, the DHCP server is usually set with:

set vci-match enable

set vci-string 'FortiSwitch' 'FortiExtender'

In the exhibit, the DHCP server for fortilink has:

set vci-match enable

set vci-string 'FortiExtender'

Because theVCI string doesn't include ''FortiSwitch'', DHCP offers are only sent to clients whose Vendor Class Identifier matchesFortiExtender. The FortiSwitch never receives an IP, so it staysOffline.

OptionBis wrong: member 'port4' matches the physical cabling in the topology.

OptionCis fine: FortiLink can be anaggregateinterface, not only physical.

OptionA(ip-managed-by-fortiipam) is unrelated; FortiIPAM isn't required here.