ATMIC NETWORKS
YOUR GUIDE TO GLOBAL CERTIFIATION

"Please note that these files may not be up to date. However, the questions will help you understand the exam format and typical question patterns."

www.atmicnetworks .com

Warning: Keep connected with our support team for latest updates

Question: 1

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

Explanation:

Zero-Touch Provisioning (ZTP) for FortiGate devices is handled throughFortiDeploy, which automatically connects a FortiGate toFortiManagerso the device can download configuration templates and be centrally managed.

For ZTP to work, the newly booted FortiGate must successfully reach FortiManager. One of thecritical requirementsis connectivity over theFGFM (FortiGate–FortiManager) management protocol, which uses:

TCP Port 541

This is clearly stated in multiple Fortinet documents:

FortiGate Cloud Admin Guidelists port541as the management channel used for FortiGate → FortiManager / FortiGate Cloud communications:"Management... Protocol: TCP, Port:541"

FortiOS Administration Guidealso confirms this:"FortiManager provides remote management of FortiGate devices overTCP port 541."

Since ZTP uses FortiDeploy to push the FortiManager IP to the device and relies on FGFM (port 541) for registration and configuration delivery,any failure on this port breaks the entire ZTP workflow.

Why option D is correct

If the FortiGate cannot reach FortiManager onTCP/541, itcannot register, cannot be authorized, and cannot receive its configuration — leading to a ZTP failure.

This is themost common causein real deployments:

Firewall blocking TCP/541

Upstream NAT device not forwarding 541

ISP restrictions

Incorrect FortiManager IP or routing issue

ZTP device behind a network that does not allow outbound 541

Why the other options are incorrect

A . The FortiGate device requires manual intervention to accept the FortiManager connection.

Incorrect.

ZTP is built specifically to avoid manual intervention. Once the FortiDeploy key is used, the device auto-connects to FortiManager without needing local acceptance.

B . ZTP works only when devices are connected using a console cable.

Incorrect.

ZTP requiresno console cable— that's the whole point. It relies on DHCP, WAN connectivity, and FortiDeploy auto-join.

C . The FortiGate device must be preloaded with a configuration file before ZTP can function.

Incorrect.

Preloading configuration defeats the purpose of ZTP.

ZTP delivers the initial configuration automatically from FortiManager using FortiDeploy.

LAN Edge 7.6 Architect Context

LAN Edge deployments often use FortiManager as the central orchestrator for:

FortiSwitch management via FortiLink

FortiAP wireless provisioning

SD-Branch configuration templates

Security Fabric automation

For all of this, ZTP enables remote sites to deploy FortiGate, FortiSwitch, and FortiAP withno on-site expertise.

If TCP/541 to FortiManager is blocked, the entire LAN Edge deployment pipeline fails, making optionDthe only valid and document-supported answer.

Question: 2

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

Explanation:

FortiLink device detection relies on FortiGate'sDevice IdentificationandIoT Detectioncapabilities to classify devices connected to FortiSwitch ports.

To enabledevice identificationandvulnerability detectionfor IoT/endpoint devices in LAN Edge deployments, FortiGate must subscribe to the correct FortiGuard services.

1. Required FortiGuard License for Device Identification (IoT Detection)

The FortiOS documentation clearly states:

“IoT detection service… requires anAttack Surface Security Rating service licenseto download the IoT signature package.”

Additionally:

“The following settings are required for IoT device detection:

A validAttack Surface Security Rating service licenseto download the IoT signature package.”

This service provides:

IoT signature package

IoT device classification

Device behavior profiling

This makesAttack Surface Securitymandatory for FortiLink device detection.

2. Required FortiGuard License for Device Vulnerability Detection

FortiOS further clarifies that IoT vulnerabilities require theIoT Detection license, which is included under the same Attack Surface service entitlement:

“To detect IoT vulnerabilities the FortiGate must have a validIoT Definitions license…”

The IoT Definitions license comeswith the Attack Surface Security Rating serviceand is used for:

Scanning connected devices

Identifying IoT/endpoint vulnerabilities

Reporting vulnerability severity

Enabling NAC-based remediation (VLAN steering, port isolation)

In LAN Edge Architect, this license combination is emphasized as a foundational requirement for:

FortiSwitch NAC

FortiLink device profiling

Automated quarantine actions

IoT device classification

Vulnerability-based segmentation

3. Why the Correct Answer Is Option D

OptionDlists:

/ FortiGuard Attack Surface Security

/FortiGuard IoT Detection

These are exactly the services required per FortiOS 7.4.1:

Attack Surface Security Rating→ provides IoT signature package + vulnerability data

IoT Detection (Definitions)→ enables actual device-type and vulnerability identification

Together they powerFortiLink Device DetectionandIoT Vulnerability Detection, which are essential LAN Edge security functions.

4. Why Other Options Are Incorrect

A . Vulnerability Management + Endpoint Protection

Not used for FortiLink device detection; Endpoint detection relies on IoT service, not FortiClient.

B . Threat Intelligence + IoT Detection

Threat Intelligence (ThreatIntel DB) is used for FAZ IOC, not LAN Edge device detection.

C . Threat Intelligence + Endpoint Protection

Same issue—does not provide IoT device classification or vulnerability scanning.

LAN Edge 7.6 Architect Context Summary

In LAN Edge designs:

FortiGate acts as the controller for FortiSwitch via FortiLink.

Device detection is done at the FortiGate level using NAC/IoT signature capabilities.

Vulnerability detection enables dynamic segmentation decisions (e.g., move device to quarantine VLAN).

To support this, two licenses aremandatory:

Attack Surface Security(includes Security Rating + IoT Detection DB)

IoT Detection(part of the same entitlement, but explicitly required for vulnerability detection)

Thus the verified answer aligns perfectly with LAN Edge operational requirements and Fortinet documentation.

Question: 3

Refer to the exhibits.

VAP configuration

■;nfi7 wireItss-controller vap edit "Corporate" set said "COIF"
set security wpa2-only-ent erpriate set auth radius
Set ;adluS"3*rve: "EAC-LibM set intra-vap-privacy enable set schedule
"always* set vlan-pooling wtp—group config vlan-pool edit 101
set wtp-grouj "rion£_l" next edit 102
set wtp-group ’Office" next
end
next end

Wi-Fi zone table

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

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

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: 4

```
config system dhcp server edit 1
        set ntp-service local
        set default-gateway 1€^254,L1
        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
```

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

Explanation:

The DHCP configuration shows:

set vci-match enable

set vci-string "FortiSwitch" "FortiExtender"

What this means

VCI = Vendor Class Identifier (DHCP option 60)

When vci-match is enabled, the DHCP server will only respond to DHCP requests from clients whose VCI string matches the configured vendor identifiers.

FortiSwitch and FortiExtender both send DHCP option 60 with:

"FortiSwitch"

"FortiExtender"

This is used in FortiLink deployments so only these devices receive IP addresses on the FortiLink network.

Therefore:

C . To connect, devices must match the VCI string; otherwise, they will not receive an IP address.

✓ Correct.

This perfectly matches FortiGate FortiLink DHCP behavior.

Summary of incorrect options

A — Ignore FortiSwitch/FortiExtender

Opposite behavior.

B — Restrict based on hostname

VCI does NOT check hostname.

D — Reserve IPs

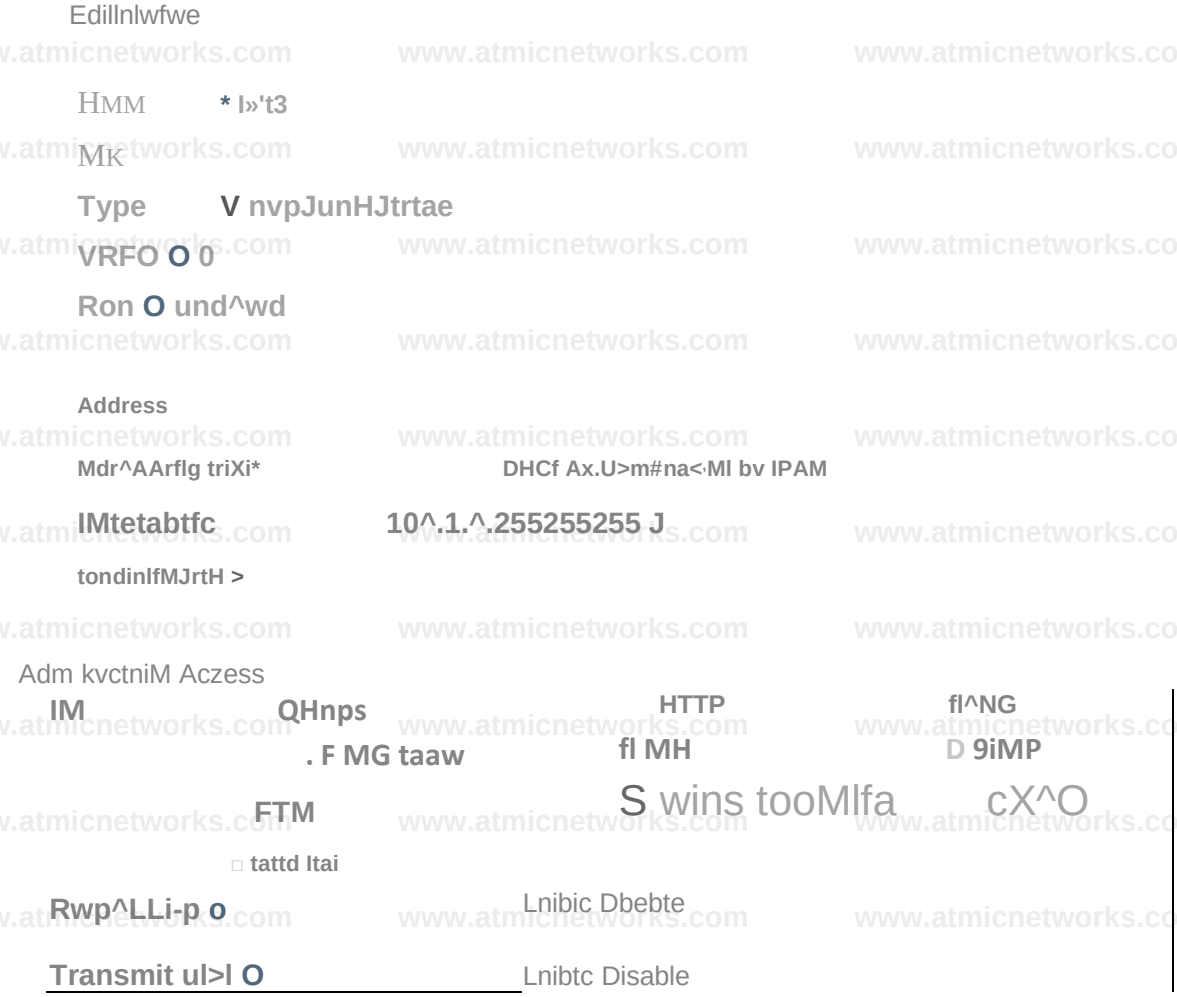
No reservation occurs; it's filtering, not reserving.

Question: 5

Refer to the exhibits.

FortiGate RSSO configuration

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 to UserName.

Answer: A,D,E

Explanation:

The problem states:

FortiGate receivesRADIUS accounting messagesonport3.

User-Nameattribute contains the username.

Classattribute contains the group membership.

Goal: authenticate users through RSSO and map them to the correct user groups.

To achieve this, three critical components must be configured:

✓A. RADIUS Attribute Value in the RSSO group must match the Class attribute

This is mandatory because:

RSSO user groups on FortiGate match users based onthe value inside the RADIUS attribute(usually Class).

For group assignment to work, FortiGate must compare:

RSSO User Group → RADIUS Class Attribute Value

This isexactly how FortiGate maps RSSO users to groups.

✓ D. RSSO agent's sso-attribute must be set to Class

Thesso-attributedefineswhich RADIUS attribute contains the group information.

Because group membership is carried in:

*Class attribute

You must configure:

config user radius

set sso-attribute Class

end

This tells FortiGate:

"Use the Class attribute to derive user group membership."

✓ E. rsso-endpoint-attribute must be set to User-Name

This identifieswhich RADIUS attributecarries the actualusername.

In this scenario:

RADIUS accounting messages contain the username inUser-Name.

So the correct setting is:

config user radius

set rsso-endpoint-attribute User-Name

end

This ensures the RSSO user object uses the correct username.

Incorrect Options Explained

B . Assign RSSO user groups to all firewall policies

Not required.

You only assign them to policies where RSSO authentication is used.

C . Device detection and Security Fabric Connection should be enabled on port3

Totally irrelevant to RSSO.

RSSO only needs RADIUS accounting, not device detection or Fabric services.

Question: 6

What is the primary function of FortiLink NAC in a LAN environment?

A. To extend security policies across FortiGate firewalls only

B. To automate device onboarding and verify security posture

C. To manage FortiSwitch devices and apply manual firewall rules

D. To ensure devices are manually placed in VLANs based on their user roles

Answer: B

Explanation:

FortiLink NACis the NAC (Network Access Control) engine built into FortiGate when it manages FortiSwitch devices.

It performs:

✓Automated device onboarding

Automatically detects new devices connecting to switches.

Uses MAC, vendor, DHCP fingerprinting, or IoT database to classify devices.

No manual VLAN assignment required.

✓Security posture verification

Works with FortiClient EMS, ZTNA tags, IoT detection.

Applies policies based on:

Device type

User role

Endpoint compliance

IoT vulnerability status

✓ Dynamic VLAN assignment

Automatically moves devices into proper VLANs, quarantine networks, or guest zones.

✓ Integration with LAN Edge & Zero Trust

Uses FortiGate + FortiSwitch + FortiAP to enforce zero-trust access.

This matches the LAN Edge 7.6 Architect explanation of FortiLink NAC.

Why other answers are wrong

A . Extend security policies across FortiGate firewalls

Not NAC. That refers to Security Fabric or SD-WAN.

C . Apply manual firewall rules

FortiLink NAC is specifically designed toautomateaccess control.

D . Manually place devices in VLANs

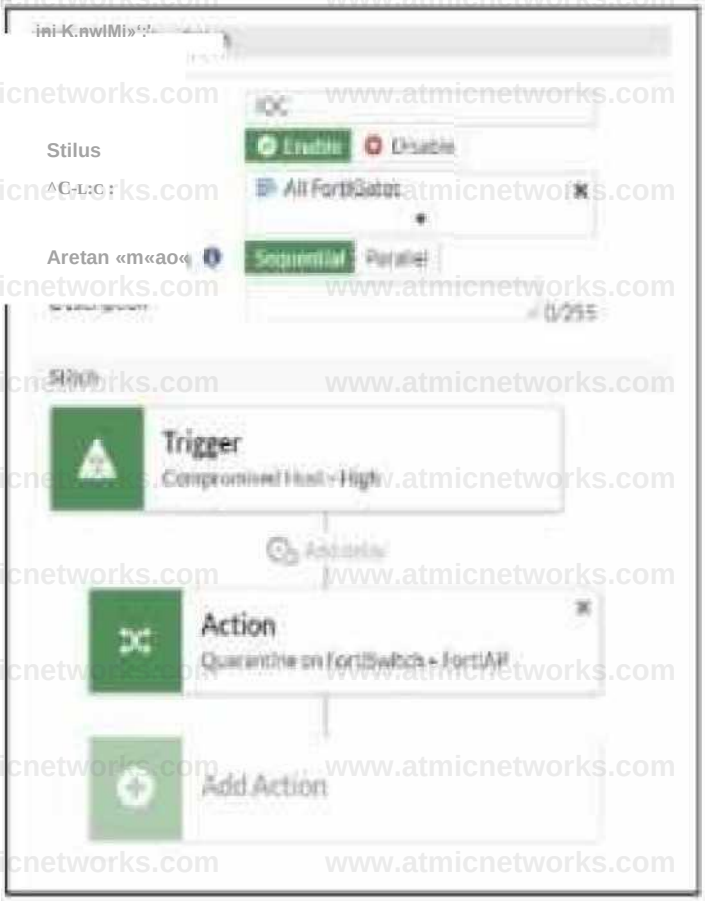
NAC eliminates manual VLAN assignment — it is dynamic.

Question: 7

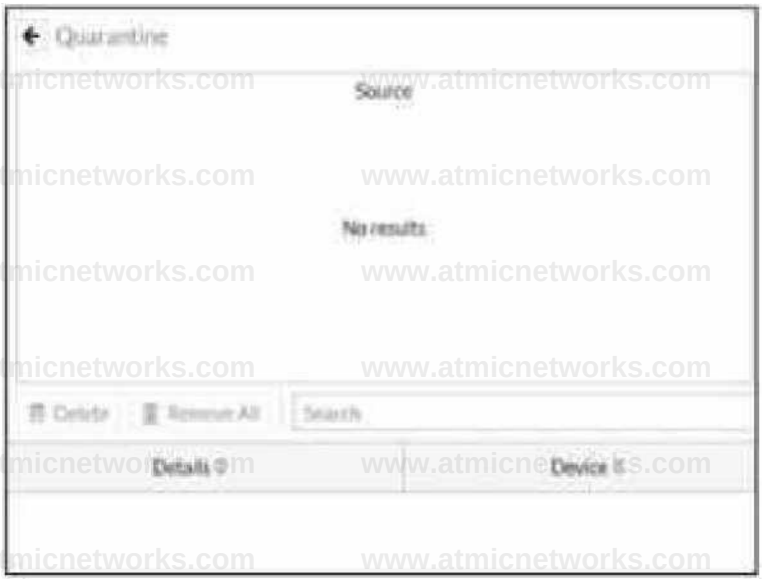
Refer to the exhibits.

FortiGate Security Fabric widget

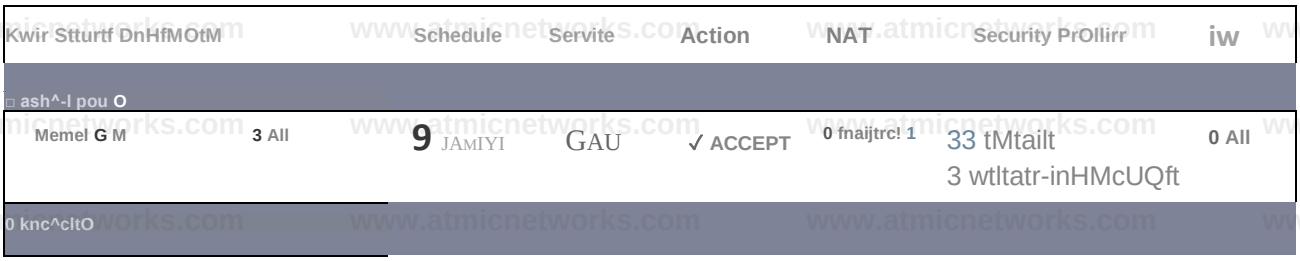
Security Fabric Automation Stitch



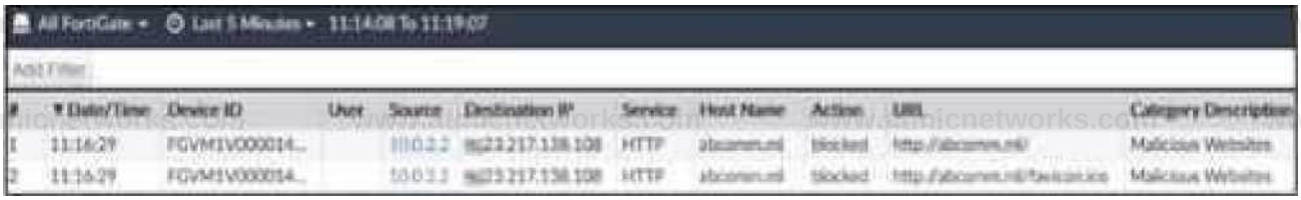
Quarantine widget



FortiGate firewall policy



ForttAnalyzer log



Examine the FortiGate configuration, FortiAnalyzer logs, and FortiGate widget shown in the exhibits.

Security Fabhc quarantine automation has been configured to isolate compromised devices automatically. FortiAnalyzer has been added to the Security Fabric, and an automation stitch has been configured to quarantine compromised devices.

To test the setup, a device with the IP address 10.0.2.1 that is connected through a managed FortiSwitch attempts to access a malicious website. The logs on FortiAnalyzer confirm that the event was recorded, but the device does not appear in the FortiGate quarantine widget.

Which two reasons could explain why FortiGate is not quarantining the device? (Choose two.)

A. The IOC action should include only the FortiSwitch in the quarantine.

B. The SSL inspection should be set to deep-Inspection

C. The malicious website is not recognized as an indicator of compromise (IOC) by FortiAnalyzer.

D. The threat detection services license is missing or invalid under FortiAnalyzer.

Answer: C,D

Explanation:

In this scenario:

FortiGate + FortiAnalyzer are part of theSecurity Fabric

AnAutomation Stitchis configured:

Trigger:Compromised Host – High(IOC from FortiAnalyzer)

Action:Quarantine on FortiSwitch + FortiAP

A test device10.0.2.1visits a malicious website.

FortiAnalyzer logs show the event, butFortiGate does NOT quarantine the device.

This means theautomation did not receive an IOC trigger, OR theFabric did not classify it as a compromise.

Let's evaluate each answer option.

C. The malicious website is not recognized as an indicator of compromise (IOC) by FortiAnalyzer.

✓ Correct.

For FortiGate to quarantine a device:

FortiAnalyzer must classify the event as aCompromised Host → High / Medium / Critical

FortiAnalyzer must generate anIOC event

FortiGate must receive that IOC through the Fabric

Even though the FAZ log shows:

Action = blocked

Category = Malicious Websites

→ That doesNOTautomatically mean an IOC was generated.

A blocked website event isnot always an IOCunless:

It is included in theIOC database

FAZ'sAnalytics / UTM / IOCengine marks it as a compromise

Thus, if FAZ only logs a "Malicious Website" event butdoes not classify it as an IOC,

Question: 8

When the MAC address of a device is placed in quarantine on FortiSwitch, what happens to its egress traffic?

A. Traffic is sent to an access VLAN.

B. Traffic is assigned to the native VLAN.

C. Traffic is sent as untagged traffic.

D. Traffic is sent to an allowed VLAN.

Answer: A

Explanation:

When a device'sMAC address is quarantinedon a FortiSwitch (via FortiLink NAC, fabric automation, or manual quarantine), FortiSwitch enforces quarantine using thequarantine VLAN, also called theaccess VLANinside FortiSwitch NAC operations.

FortiSwitch behavior is defined in LAN Edge documentation:

Quarantined devices are moved into an"access VLAN" reserved for isolation.

This VLAN isstatically defined on the FortiGate NAC policy, and switch ports dynamically reassign the quarantined MAC into that VLAN.

All egress traffic from the quarantined MAC is forced into this VLAN, preventing access to the production network.

Thus, the correct description is:

✓Traffic is sent to an access VLAN.

Options B, C, and D are incorrect because:

Quarantine doesnotreassign to native VLAN.

It doesnotsend untagged traffic arbitrarily.

It doesnotforward traffic to allowed VLANs

Question: 9

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

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: 10

Why is it critical to maintain NTP synchronization between FortiGate and FortiSwitch when FortiLink is configured?

A. To facilitate synchronization of firmware updates across devices

B. To allow FortiSwitch to communicate with other FortiSwitche devices in the network.

C. To ensure accurate time for logs, authentication, and event correlation

D. To allow FortiSwitch to function in standalone mode if FortiGate becomes unavailable

Answer: C

Explanation:

FortiGate and FortiSwitchmust share synchronized timewhen operating in FortiLink mode.

Documented reasons in FortiOS:

Accurate time synchronization is required for logs, authentication events, and fabric correlations.

Why it's critical:

802.1 X EAP and RADIUS timestamp validation

NAC policy enforcement timestamps

Certificate validation

Log correlation in Security Fabric / FortiAnalyzer

Incorrect options:

A: Firmware synchronization does NOT require NTP.

B: Switch-to-switch communication does not depend on NTP.

D: Standalone mode is unrelated to time sync.

Question: 11

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. 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: 12

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: 13

Refer to the exhibits.

SSL-VPN settings

SSI-VPN Settings

Connection Settings 0

Enable SSL VPN C

Listen on Interfaces) ■ port? X

\+

Listen on Port 10443

A Web mode access will be listening at
W httLS^RJOZuV^^

Server Certificate If vpn *

Rett reel HTTP to SSL VPN O

Restrict Access | Limit access to specific hosts

Idle Logout O

Inactive Fea 300 - Seconds

Require Client Certificate C

Real-Time debug output

```
FortiGate 5 diagnose debug application fnbamd -1
Debug messages will be on for 30 minutes,
FortiGate 2 diagnose debug enable

FortiGate 2 [2341] handle_req-Rcvd auth_cert req id=1280O58918, len-1104, opt=0
[940]   cert_auth_ctx_init-req_id=12830SS918, opt=0
[103]   cert_chg_st- 'Init'
[140] fnbamd cert load certs from req-1 cert(si in req.
[99]   cert_chg_st- 'Init' -> 'Chain-Build'
[693] _cert_build_chain-req_id=1288058918
[200] fnbamd chain build-Chain discovery, opt 0x1", cur total 1
[216] fnbamd_chain_buiId-Following depth 0
[271] fnbamd_chain_build-Extend chain by system trust store, (no luck)
[203] 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]  ce rt_ca_query_do_next-re q_id=l2 8 8058919
[99]   cert chg st- 'CA-Query' -> 'Validation'
[804] _cert verify-req_id~12B8058918
[805] cert verify—Chain ia not complete.
[200] fnhamd_chain_build-Cham 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
[4101 fnbamd_cert_verify-Following cert chain depth 0
[676] fnbamd_cert_check_group_li3t-checking group with name 'SS17PN'
[490]   check_add_peer-check 'student'
[460]   quxck check neer-CA does not match.
[498]   check add_peer-'student' check ret:bad
[193] get default ocsp CtM-def ocsp ctx~(nil). no corp query-0, ocsp enahled=0
[841] cert rertfy.do_next-req_id=1288058918
[99]   cert_chg st- 'Validation' -> 'Done'
[886]  _cert_done-req_id=12B8058918
[1652] fnbamd_auth_ses3ion_done-3es3ion done, id=1288058918
[931]  _fnbamd_cert_auth_run-Exit, req_id=1288058918
[1689] create_auth_cert_3ession-fnbamd_cert_auth_init returns 0, id-1288058918
[1608] auth_cert_success-id=1280058918
[1031] fnbamd cert_auth copy cert statua"req_id=12B8058918
[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_statu3-issuer of cert depth 0 is not deteced in CMDB.
[1158] fnbamd_cert_auth_copy_cert_status-Cert st 2040, req_id=128805891B
[217] fnbaffld_com_send_result-Sending result 0 (nid 672) for req 1288058918, len=2144
[1553] de3troy_auth_cert_ses3ion-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.

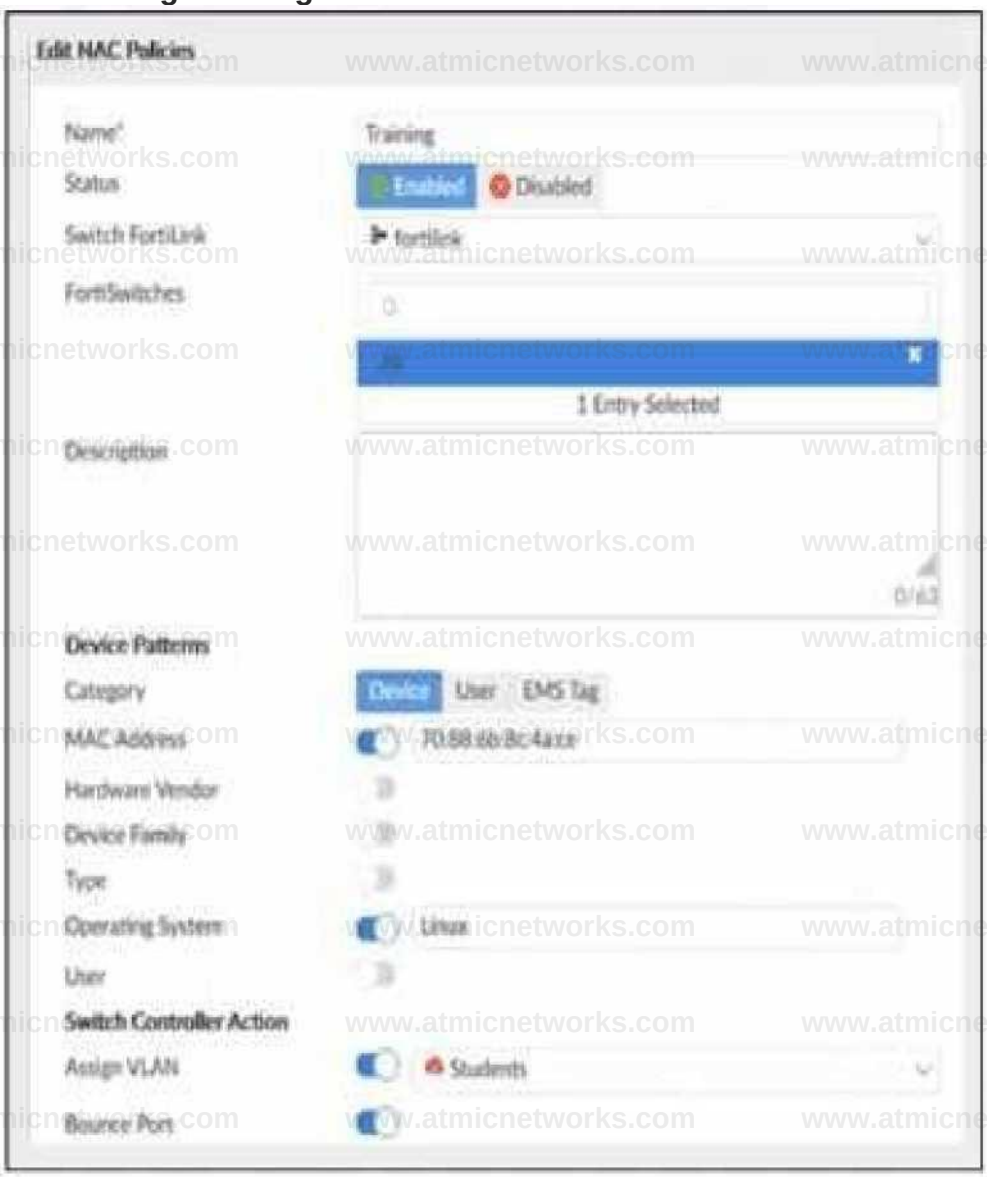
C . Set the user certificate as the Server Certificate– incorrect; server and client certificates serve different roles.

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: 14

Refer to the exhibits.

FortIManager configuration



FortiGate CLI output

```
FoitiGatcf diagnose switch-controller switch-info mac-table S224EPTF19005867
▼don: root

Managed Switch : 3224EPTF19005867 0

MAC: 00:0c:29:e€:ea:d2 VLAN: 4089 Trunk: GVM1V00OO1416B0(trunk-id 0)
    Flags: 0x000104cl ( hit trunk dynamic arc-hit native ■

MAC: 00:0c:29:e6:ea:d2 VLAN: 1 Trunk: GVM1V0000141680(trunk-id 0)
    Flags: 0x000104cl ( hit trunk dynamic arc-hit native I

MAC: 00:0c:29:e€:ea:d2 VLAN: 4093 Trunk: GVM1V0000141680(trunk-id 0)
    Flags: 0x000104cl ( hit trunk dynamic arc-hit native )

MAC: 00:0c:29:e6:ea:d2 '.'LAN: 4 094 Trunk: GVM1V00O0141680 (trunk-id 0)
    Flags: £x000104cl < hit trunk dynamic arc-hit native )

MAC: 7Q:88:6b:8e:4a:ce VLAN: 40B9 Port: port2(port-id 2)
    Flags: 0x00010441 l hit dynamic src-hit native )

MAC: 04:15:90:3o:«7:80 VLAN: 1 Port: portl (port-id 1)
    Flags: 0x00010441 ( hit dynamic src-hit native )

MAC: 00:Oc:29:06:ea:d2 VLAN: 4088 Trunk: GVX1V000014168D(trunk-id 0)
    Flags: 0x000104cl < hit trunk dynamic src-hit native )

MAC: 00:0c:29:«6;ea:d2 VLAN: 10 Trunk: GVMlv0a00141680(trunk-id Oi
```

```
    Flags: 0x003104c1 ( hit trunk dynamic src-hit native )

  Total Displayed: 8

FortiGate! diagnose switch-controller mac-device nac   onboarding
vdoa: root
VLAN 4089  MAC                 LAST-SEEN     TYPE      LOCATION
           70:88:6b:8c:4a:ca   4             3*        S224EPTF19005B67       port2

FortiGate! diagnose switch-controller mac-device nac   known
vdom: root
MAC        LAST-KNOWN-SWITCH     LAST-KNOWN-FORT         MATONED~NAC-POLICY MAC-PCLIOY- ACT TON    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. Q 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. Q 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. X 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. X Not the cause here.

Question: 15

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.

Question: 16

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

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: 17

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

Explanation:

In user certificates used with FortiGate / FortiAuthenticator / SSL-VPN / 802.1X, the following attributes are important:

Subject field & UPN

Provide a unique identity for the user (CN and/or UPN).

FortiGate can use theSAN/UPNfield for LDAP-integrated certificate authentication.

Expiration date

Limits how long the certificate is valid, enforcing lifecycle and rotation.

CRL URL & OCSP URL

Tell FortiGate (or any relying party)where to check if the certificate has been revoked.

Enablesnear real-time revocationusing OCSP or periodic CRL downloads instead of relying only on expiration.

By carefully configuring these fields:

The certificate uniquely and correctly identifies the user.

Relying systems can performaccurate and timely revocation checks, improving security.

Why other options are wrong:

A: It does the opposite—CRL/OCSP increase automation, not manual revocation.

B: These attributes do not inherently limit a cert to specific devices; that's done via key usage, EKU, or device certs.

D: They don't "ensure universal validity"; they make the certprecisely boundto one identity with enforceable lifetime and revocation.

Question: 18

Refer to the exhibits.

FortiAuthenticator

Interface: port!

S La Lus 0

IPv4 10 01.150/255 255 255 0

IPv6:

A dm tn access:

t SSH (TCP/22)

HTTPS (TCP/443)

OGUHTCP/4431

OREST API i/aoi/)

O' Fabric (/api/vl/fabric/]

J SNMP (UDP,161)

CHTTP(TCP/BO)

Services-

C HTTPS (TCP/443)

< "' legacy Sell -service Portal (/login/)

O' Capbve Portals (/guests, /portal)

OSAML HP(/MmMdp)

O SAML SP SSO (/wml so, /hgin/samlauth)

< ' Kerberos SSO 1/login/kerb-auth)

< ' SCEP (Zapp/cert/sCep)

OCRL Downloads (Zapp/cert/cH)

> CMP (/app/cert/cmp2/J

< FortiToken Mobile API Oapi/vl/ousnauinresp. /api/vl/transfertoken)

C OAuth Service (/ap*/vi/oauth. /api/vl,'pushpoll. /guests, /portal) r HTTP rrcp/eo)

C SCEP (/app/cert/scep)

O CRL Downloads (/app/cert/cr!)

1 CMP (/app/cert/cmp2/l

> SAML MP metadata (/saml-idol

C Kerberos SSO (/login/kerb auth)

& RADIUS Accounting Monitor (UDP 1646)

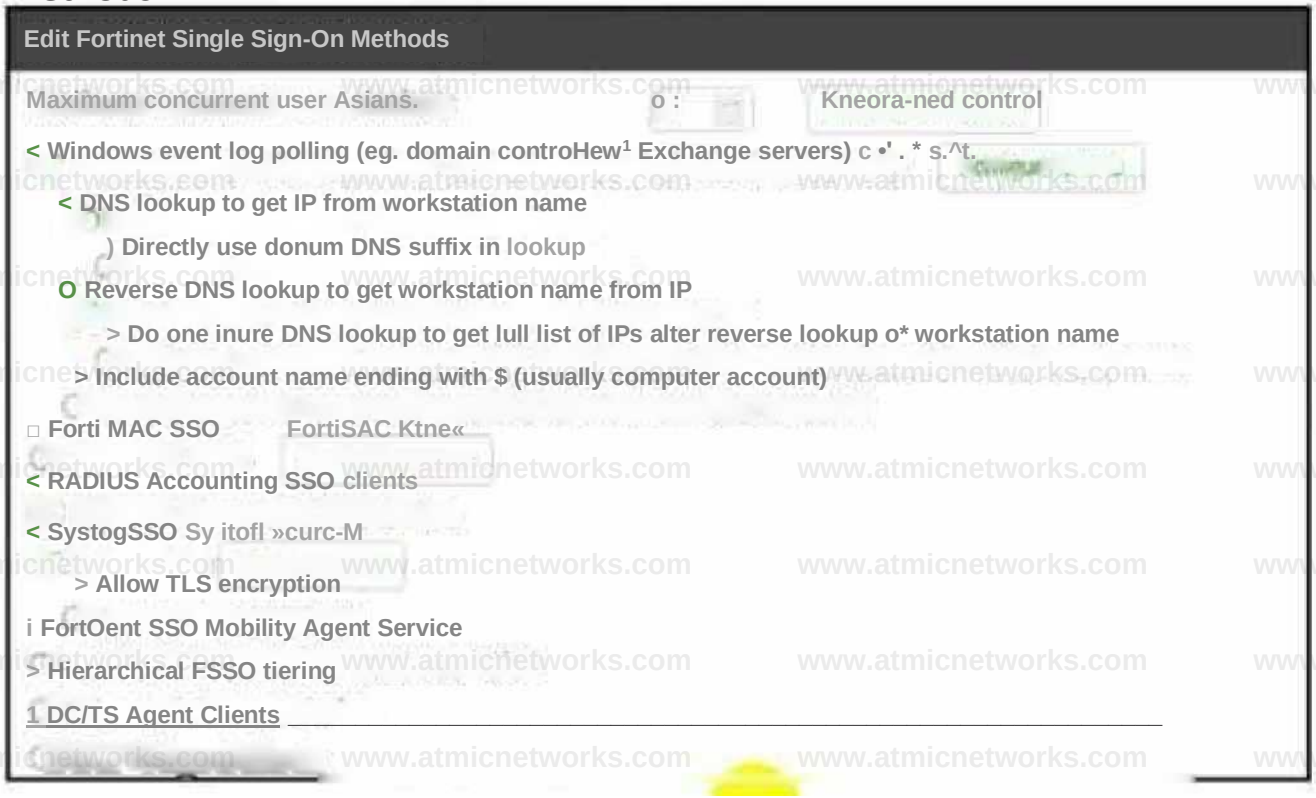
< RADIUS Auth (UDP/1812)

> RADIUS Accounting SSO (UOP/1813)

> RADSEC {TCP/2083)

> TACACS* Auth (TCP/49)

FortiAuthenticator SSO Methods



FortiAuthenticator RADIUS Accounting SS Client

A company has multiple FortiGate devices deployed and wants to centralize user authentication and authorization. The administrator decides to use FortiAuthenticator to convert RSSO messages to

FSSO, allowing all FortiGate devices to receive user authentication updates.

After configuring FortiAuthenticator to receive RADIUS accounting messages, users can authenticate, but FortiGate does not enforce the correct policies based on user groups. Upon investigation, the administrator discovers that FortiAuthenticator is receiving RADIUS accounting messages from the RADIUS server and successfully queries LDAP for user group information. But, FSSO updates are not being sent to FortiGate devices and FortiGate firewall policies based on FSSO user groups are not being applied.

What is the most likely reason FortiGate is not receiving FSSO updates?

A. The RADIUS Username and Client IPv4 attributes are not defined on FortiAuthenticator.

B. The LDAP server is not configured to retrieve group memberships for RSSO users.

C. FortiAuthenticator is missing the FSSO user group attribute in the configuration.

D. The FortiAuthenticator interface is not enabled to receive RADIUS accounting messages.

Answer: A

Explanation:

In this design, FortiAuthenticator receivesRADIUS accounting (RSSO) messages, looks up the user in LDAP to get group information, theninjects FSSO logon eventstoward all FortiGate devices.

From the exhibits we know:

FortiAuthenticatoris receiving RADIUS accountingfrom the RADIUS server.

LDAP queries are successful and return group membership.

But FortiGatedoes not receive FSSO logons, so identity-based policies are not applied.

For FortiAuthenticator to create an FSSO logon, the RADIUS accounting record must be correctlyparsed into at least:

Username

Client IP address

These are mapped from the RADIUS attributes in theRADIUS Accounting SSO clientconfiguration (for example, User-Name and Framed-IP-Address). If these are not defined or mapped incorrectly, FortiAuthenticator can see the accounting packet butcannot build a valid FSSO session, so no update is sent to FortiGate.

Thus the most likely root cause is:

✓The RADIUS Username and Client IPv4 attributes are not correctly definedfor that RADIUS Accounting SSO client (optionA).

Other options conflict with the scenario:

B– LDAP is already successfully returning groups.

C– FSSO user group attribute is separate; even without it, FSSO logons would still be created (just without group mapping).

D– The interfaceisreceiving RADIUS accounting, so it is clearly enabled.

Question: 19

What is the expected behavior when enabling auto TX power control on a FortiAP interface?

A. FortiGate monitors the signal strength of nearby AP interfaces and adjusts its own transmit power every 30 seconds to match the signal strength of the adjacent AP

B. FortiGate measures the signal strength of nearby FortiAP interfaces every 30 seconds and adjusts their transmit power to ensure they remain detectable at -70 dBm.

C. FortiGate periodically measures the signal strength of the weakest associated client and adjusts the AP radio power to align with the detected signal strength of that client.

D. The AP periodically evaluates the signal strength of its own transmission from the client perspective and adjusts its power to ensure the signal is detected at -70 dBm.

Answer: C

Explanation:

Auto TX power control on FortiAP is an RF-optimization feature:

FortiGate (as wireless controller) continuously evaluatesRSSI of associated clientson each FortiAP radio.

The algorithm focuses on theweakest client(the one with the worst signal) and adjusts the AP's transmit power so that this client's signal level stays within a configured / target range.

This helps balance coverage and limit co-channel interference: APs don't transmit at maximum power when clients are close, but will increase power when the weakest client signal drops too low.

Therefore the correct behavior description is:

✓C- AP power is adjusted based on the weakest associated client's signal.

Why the others are wrong:

AandBtalk about matching nearby APs' power or forcing everything to –70 dBm, which is not how FortiAP auto TX works.

Dincorrectly states the AP "evaluates its own transmission from the client perspective"; the AP can only infer client-side conditions from theclient's RSSI at the AP, not the inverse.

Question: 20

Refer to the exhibits.

FortiGate VLAN AP settings

™t^g system interface edit "AFa" act cdoi "roflt* JVC it ID. 1G. LCG.Z^ 35S.Z-55.2S5.5 pet ailowaccajs [itg wt alias *AP HanagenenL* a Ct It vi cr ■ ide ritxf i-i a t LC n t nat Lt act tele 3 an act a^tep-index 11" act ip-.manage 2-ty-fs"i ipac: disable st: interface "fortlimit" aet Timid LOu next end

DHCP configuration

config system dhep sei ver edit 7 set ins-strvice default act Stfanlt-gatewty uJ 2. x.jJ^i* sec nezualc 255.255,25=.0 net interface *APs* contig ip-zuge edit 1

BEL start-ip 10.L0.1004 set end-ip JO.iO ,irjQ>253 next end nut end

FortiSwitch portl VLAN AP assignment

```
;onfl^ switch-controller managed-switch
    edit "FortiSwitch*
        see sr. •522<EFm8006ai4w
        aet fsw-wanl-peex "fortxlink*
        set fsw-wanl-admin enable
        aet poe-dewcticn-type 2
        aet version 1
        set max-allowed-trunk-members 9
        aet pre-prcrviaioped 1
        set dynamic-capability DxOOOOOOOOOW>DOOOi5S102Tr$7dddf£f7 •confxg ports edit
        "parti"
                set pee-capable 1 set vlan ”Aps*
                set cllowed-vlans "VLANIOZ" “VLANiui" "quarantine set unrigged-vlans
                "quarantine* set export-to "root"
                set Etac-addr 0< J d5: SO: 39:7d: 9e 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

Explanation:

From the exhibits:

Interface“APs”is a VLAN sub-interface onfortilinkwith IP10.10.100.254/24and a DHCP server scope 10.10.100.1–10.10.100.253.

This VLAN is assigned toport1on the managed FortiSwitch for FortiAPs.

The interface config showsonly allowaccess ping—Security Fabric Connection is not enabled.

In LAN Edge designs, FortiAPs connected through FortiSwitch are discovered and managed asLAN edge devices of the Security Fabric. FortiOS documentation states that FortiAPs and FortiSwitches appear in the Fabric topologyonly when connected on an interface with Security Fabric Connection enabled.

If the VLAN/AP management interface lacksSecurity Fabric Connection:

FortiGate does not treat that network as aFabric connection segment.

CAPWAP discovery from FortiAPs on that VLAN will not result in the AP being onboarded and shown for management.

Therefore the key misconfiguration is:

E. - Security Fabric is disabled on the VLAN interface used for AP management.

Why the others are not the root cause:

B . Firmware incompatibility– would usually show as a “Managed (upgrade required)” or similar status after discovery, not complete non-detection. The scenario specifically points to a configuration issue, not firmware.

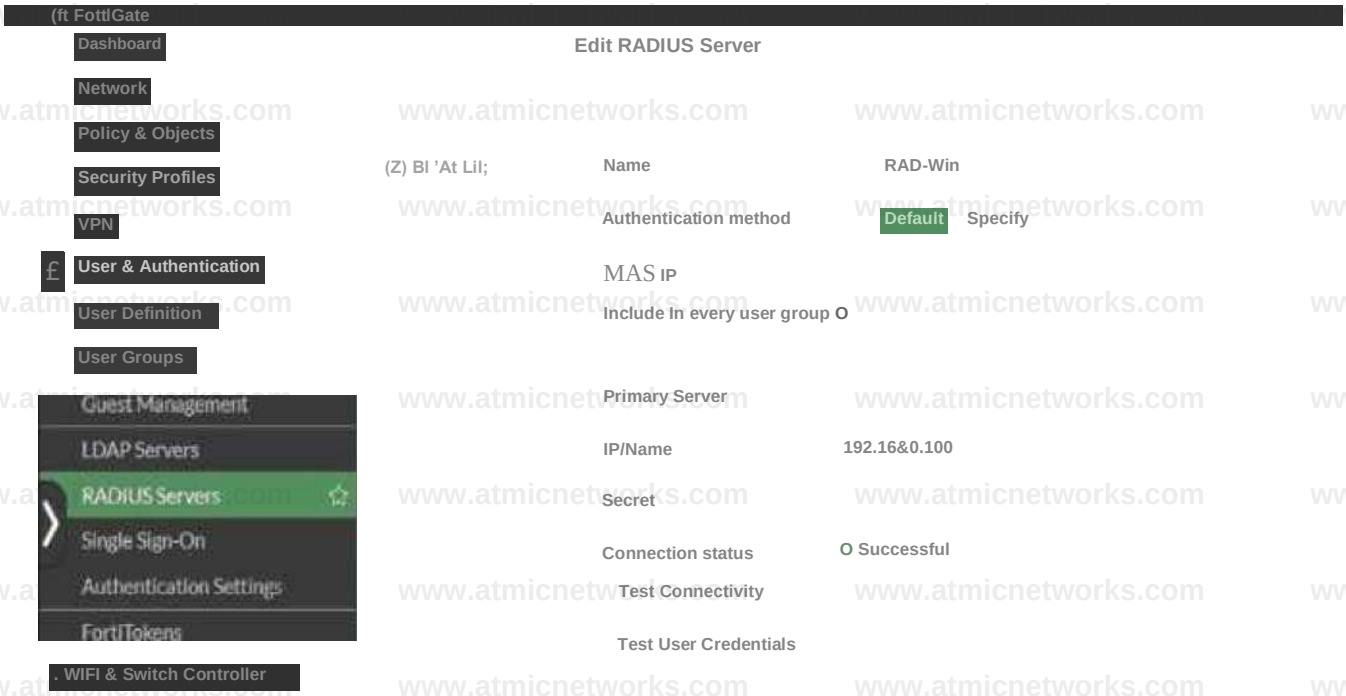
C . VLAN not tagged correctly on uplink– The FortiSwitch uplink to FortiGate is the FortiLink trunk, and the VLAN sub-interface APs is already bound to fortilink, so tagging on the uplink is correct by definition.

D . CAPWAP ports not open– CAPWAP (UDP 5246/5247) is terminated locally on FortiGate and does not depend on any firewall policy; these ports are open on the FortiGate itself by default.

Question: 21

Refer to the exhibit.

RADIUS Server configuration



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: A,D

Explanation:

Question: 22

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: A,D

Explanation:

Goal: enforce captive portal authentication overHTTPSfor guests.

On FortiGate/FortiAuthenticator captive portal setups:

HTTP redirectis used so that when a guest browses to any HTTP site, their request is redirected to theportal URL.

Theportal URLitself must beHTTPSif you want a secure login page.

FortiOS captive portal and firewall authentication guidelines recommend:

EnablingHTTP redirectso unauthenticated HTTP traffic is transparently sent to the portal.

Configuring theportal URL with HTTPS, often referencing a certificate on FortiGate or FortiAuthenticator.

Therefore:

A . Enable HTTP redirect in the user authentication settings. ✓This ensures unauthenticated HTTP requests are redirected to the (now HTTPS) portal.

D . Update the captive portal URL to use HTTPS on FortiGate and FortiAuthenticator. ✓This makes the login itself secure (TLS-protected).

Incorrect:

B– You don’t need a new SSID; the same SSID can use HTTPS portal.

C– Disabling HTTP admin access on the SSID doesn’t control the captive portal scheme; HTTPS enforcement is done by the

portal configuration and redirect, not by admin-access flags.

Question: 23

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

Explanation:

In FortiLink NAC for LAN Edge:

When a device first connects, it is placed into theonboarding VLAN.

NAC policies then classify the device (by MAC, OS, user, EMS tag, etc.).

If a NAC policy matches, the device may be moved to anaccess VLANorquarantine VLAN.

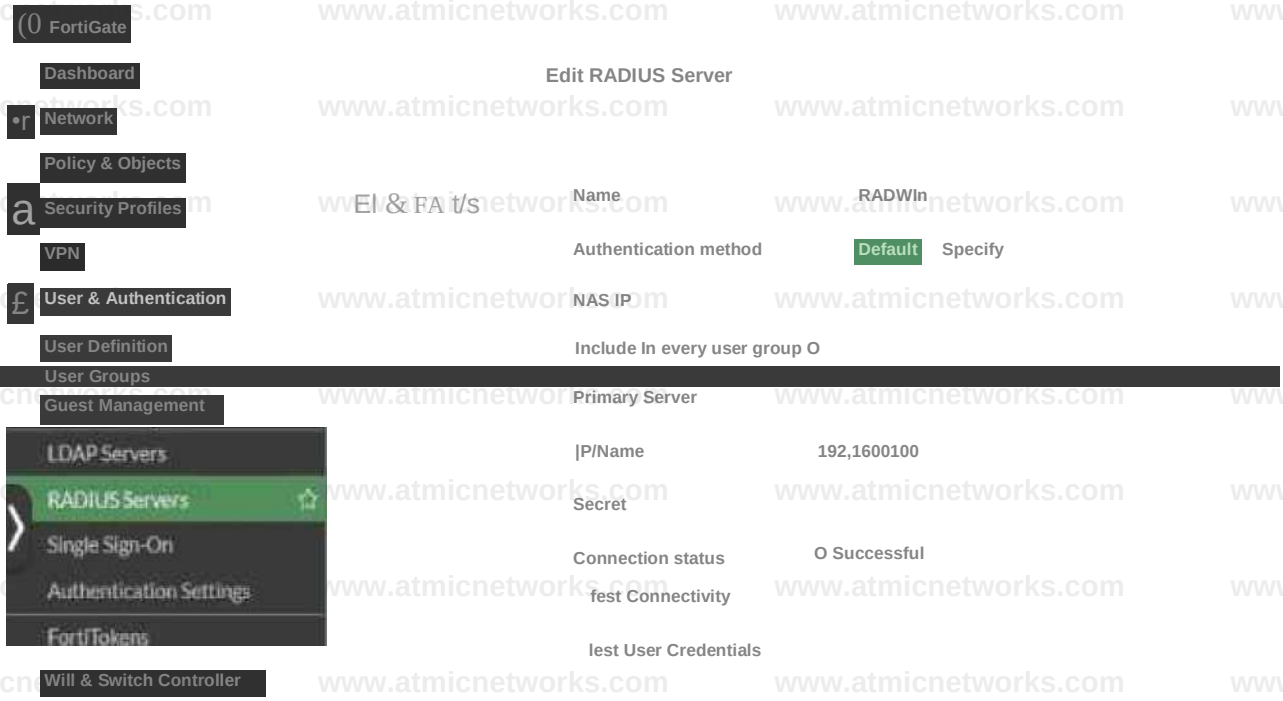
Ifno NAC policy matches, the device simplystays in the onboarding VLAN.

FortiOS / LAN Edge documentation describes the onboarding VLAN as thedefault VLAN for unknown or unclassified devices, until NAC policy evaluation moves them elsewhere.

Question: 24

Refer to the exhibit.

FortiGate Radius Server

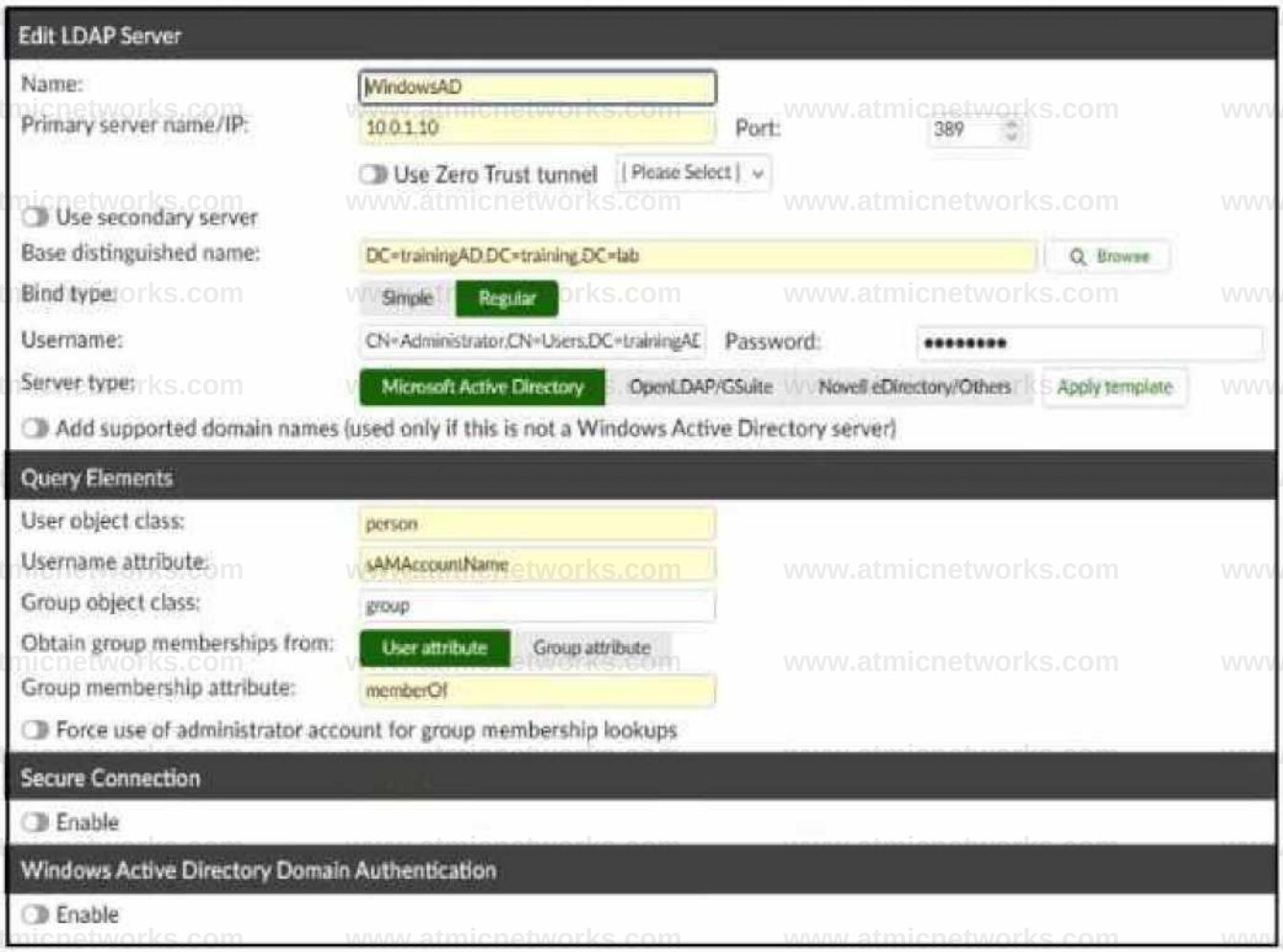


FortuiGate CLI RADIUS server test

```
FortiGate t
FortiGate I diagnose teat authserver radius FAC-Lab pap wifilOl password authenticate •wifilOl• against 'pap* succeeded, server-primary aaaigned_rad_aesaion_id-197182fl0639473
aesalon_tuneout-0 aeca ldle_tlaeout'0 secs'

FortiGate I diagnose teat authserver radius FAC-Lab mschap2 wifi 101 password authenticate *wifU01* against *mschap2' failed, assigned_rad session id-19718280638474 session tioeout-0
secs Idle timeout-0 sees!
```

FortiAuthenticator - Remote LDAP server configuration



A RADIUS server has been successfully configured on FortiGate, which sends RADIUS authentication requests to FortiAuthenticator. FortiAuthenticator, in turn, relays the authentication using LDAP to a Windows Active Directory server.

It was reported that wireless users are unable to authenticate successfully.

The FortiGate configuration confirms that it can connect to the RADIUS server without issues.

While testing authentication on FortiGate using the command diagnose test authserver radius, it was observed that authentication succeeds with PAP but fails with MSCHAPv2.

Additionally, the Remote LDAP Server configuration on FortiAuthenticator was reviewed.

Which configuration change might resolve this issue?

A. Change the RADIUS authentication protocol to CHAP

B. Enable Windows Active Directory Domain Authentication.

C. Manually add user credentials to the FortiAuthenticator local database

D. Use RADIUS attributes under the FortiGate configuration.

Answer: B

Explanation:

From the exhibits and text:

FortiGate →RADIUS→ FortiAuthenticator

FortiAuthenticator →LDAP→ Windows AD

diagnose test authserver radius ... papsucceeds

diagnose test authserver radius ... mschap2fails

This behavior matches a classic limitation documented in FortiOS:

When usingLDAPas the back-end, the RADIUS server must usePAP. CHAP/MS-CHAPv2 arenot supportedwith plain LDAP because the server cannot validate the challenge–response without access to password hashes.

In the Remote LDAP server config on FortiAuthenticator, the option"Windows Active Directory Domain Authentication" is disabled.When this feature isenabled, FortiAuthenticator can talk to AD usingKerberos/NTLMinstead of a simple LDAP bind, whichdoes support MS-CHAPv2for incoming RADIUS authentications.

So to allow MS-CHAPv2 all the way from FortiGate to AD, you must:

Keep FortiGate using RADIUS with MS-CHAPv2 → FortiAuthenticator

EnableWindows Active Directory Domain Authenticationso FortiAuthenticator can properly validate MS-CHAPv2 against AD.

Why the other options are wrong:

A . Change to CHAP– CHAP still cannot be validated over LDAP; docs say LDAP back-ends must usePAP.

C . Manually add users to local DB– That would allow local-DB auth but does not fix MS-CHAPv2 against AD.

D . Use RADIUS attributes on FortiGate– Attributes do not influence the EAP inner method; they don't fix MS-CHAPv2 failures.

Therefore the configuration change that can realistically fix the MS-CHAPv2 problem isenabling Windows Active Directory Domain Authentication on FortiAuthenticator (B).

Question: 25

Refer to the exhibits.

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

Explanation:

In a LAN Edge deployment:

FortiSwitch is managedthrough FortiGate via FortiLink.

FortiAIOps integrates withFortiGateas the single managed device; from there it gains visibility intoall Fabric and LAN-edge devices(FortiSwitch, FortiAP) that are registered to that FortiGate.

Once the FortiGate is successfully added to FortiAIOps (as shown in the exhibit, statusOnline / Successfully Discovered), all FortiSwitches managed by that FortiGate are:

Discovered automatically through the FortiGate–FortiAIOps connection

Shown under the appropriate inventory / switch views withno separate onboarding stepfor each switch.

This is why no extra IP, serial number, or credential entry is required for FortiSwitch.

So:

AandBsuggest manual per-switch onboarding, which is not how FortiAIOps works with LAN Edge.

Dsimilarly assumes direct FortiSwitch management, but FortiAIOps talks toFortiGate, not the switch.

Therefore the correct behavior is that theFortiSwitch is added automatically (C)once its managing FortiGate is connected to FortiAIOps.

Question: 26

Refer to the exhibit.

WTP profile configuration

contig wireless-cantroller wcp-profil? edit 'S.niF' config platform sit type 231F
end set handoff-rasi 30 set har-ioff sts- thresh 30 oet ap-cotiBtry US zSnJEig iodio-1 set band 3J2.Iln-20 net wlds-pxoflle "default-wid9-apscan-enabled" set vap'-all manual set vaps "StudentO!" act channel "1" *€" "11" end cMfig tadie-2 set band 802.11ac-SG sec thditrtel-bDndliig WtHt set vids prcfile "default wide-tap jean'-dhabled[1]* set darep enable net cLrp-p:_ilie "drip-default" set TOP-CU manual set vapa "StudentGl" set channel *36" "^^" *52* end ■config radios set node disabled
end
text
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 - 3 3 dBm signal strength. The second AP measures the new client at -43 dBm signal strength.

If the new client attempts to conned 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

Explanation:

From theWTP profile:

set handoff-rssi 30

set handoff-sta-thresh 30

config radio-1

set band 802.11n-2G

set vaps "Student01"

config radio-2

set band 802.11ac-5G

set darrp enable

set arrp-profile "arrp-default"

set vaps "Student01"

Key points:

Same SSID (Student01)is broadcast onboth APsand onboth bands(2.4 and 5 GHz).

handoff-sta-thresh 30 enablesclient load-balancingbetween APs:

When an AP radio hasmore than 30 associated clients, it starts rejecting new associations so that clients connect to a neighboring AP instead (as long as RSSI is still acceptable).

Current client counts:

AP1:32 clients on 5 GHz, 22 on 2.4 GHz

AP2:12 clients on 5 GHz, 20 on 2.4 GHz

So on 5 GHz:

AP1's 5-GHz radioexceedsthe 30-client threshold (32 > 30) → it will try topush new clients away.

AP2's 5-GHz radio iswell belowthe threshold (12 clients) and will happily accept new clients.

The new dual-band client is seen at:

–33 dBmby AP1

–43 dBmby AP2

Even though AP1 has the stronger signal, its 5-GHz radio is already overloaded according to the configured threshold, so AP1 will refuse association attempts from that client. The client will then associate toAP2's 5-GHz radio, which:

Hasfewer clients(better airtime per device), and

Still has an acceptable signal (–43 dBm is easily usable on 5 GHz).

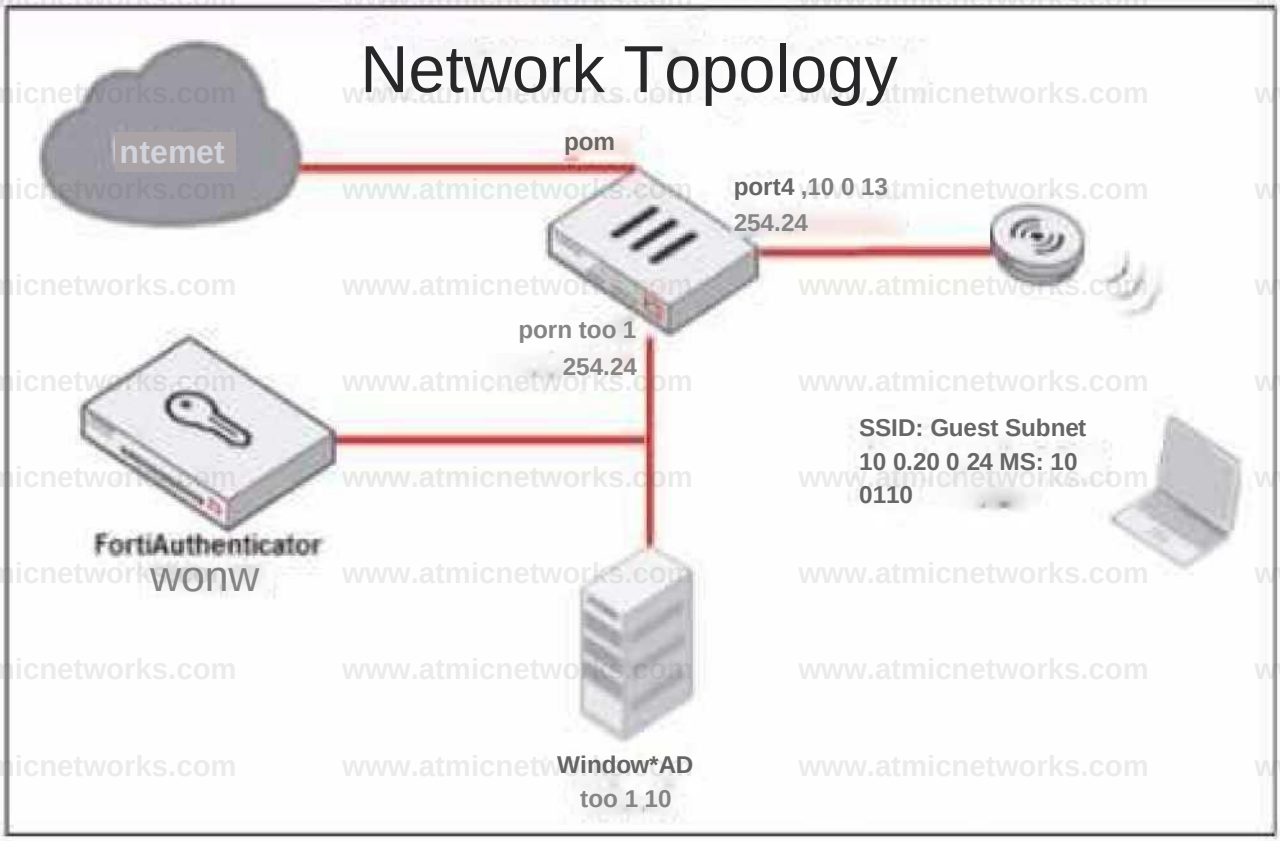
That matches optionCexactly.

Other options are incorrect because they ignore the configuredclient-load-balancing thresholdsand assume association based purely on RSSI or prefer 2.4 GHz, which is not what this profile is tuned to do.

Question: 27

Refer to the exhibit.

Network Topology



WiFi settings

WiFi Settings

SSID Guest

Client limit O

Broadcast SSID €

Beacon advertising □ Name 0 Model 0 Serial number

Security Mode Settings

Security mode Open *

Captive Portal O

Portal type Authentication •

Authentication portal Local I

http$^actrainlngad.uainlngJab£ue$^

User groups M guestportal x

4

Exempt sources

Exempt destinations/servlces Q FortlAuthenticator x

5 WindowsAD ^ x

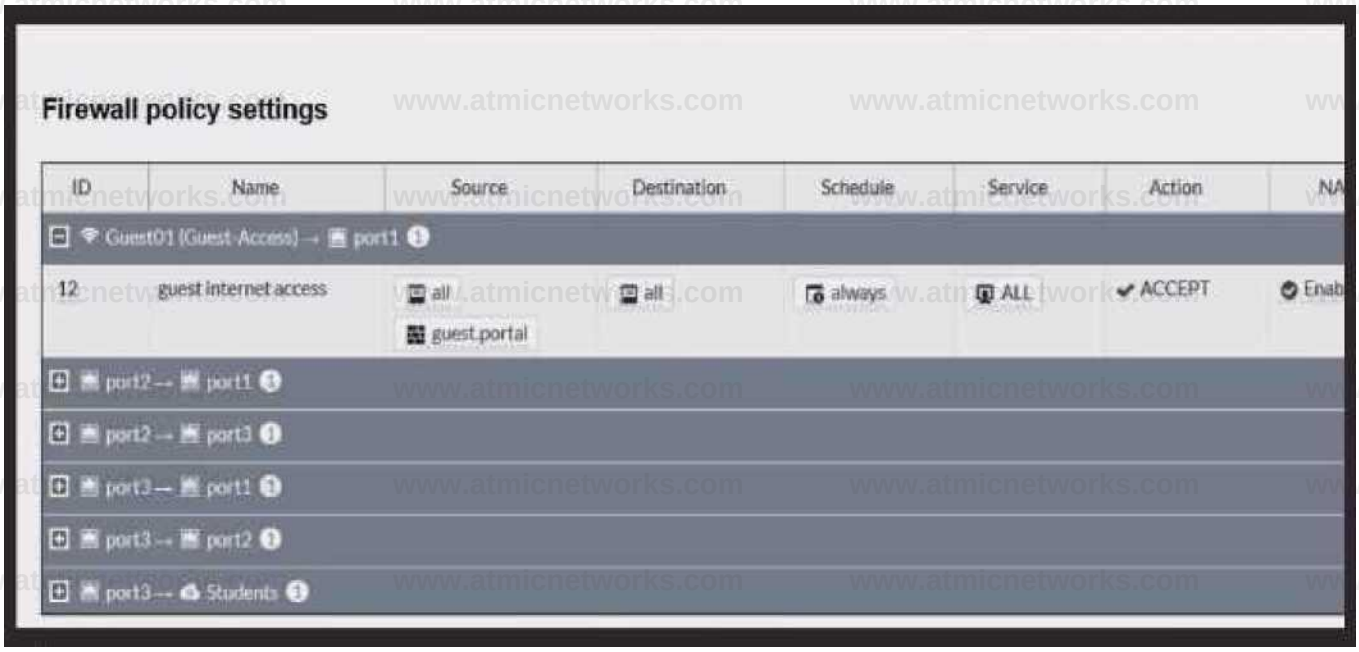
♦

Redirect after Captive Portal l >ri?.!i.)i Pi-qtRrbt

Client MAC Address Filtering

RADIUS server *

Address group policy Disable Allow Deny



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

Explanation:

From the exhibits:

SSID “Guest”

Security mode:Open

Captive Portal: Enabled, portal typeAuthentication → External

External portal URL: https://fac.trainingad.training.lab/guest (FortiAuthenticator)

Exempt destinations/services:FortiAuthenticator and WindowsAD

Firewall policy

From theGuest interface/zonetoport1 (Internet)

Source user group:guest.portal(authenticated users)

The flow for anexternal captive portalis:

Client associates to theopen Guest SSID.

Client makes an HTTP(S) request.

FortiGate intercepts and redirects the client to theexternal portal.

Client must be able toreach FortiAuthenticator's IP(and AD if the portal needs it)before authentication.

In this setup:

Theexempt destinationsetting tells the captive portal logicnot to require authenticationfor traffic going to FortiAuthenticator and WindowsAD.

However, there still must be a firewall policy that allows traffic from the Guest SSID subnet to those exempt destinations.

The existing firewall policy uses theguest.portal user groupas a source condition, which only matchesaftersuccessful portal authentication. Before login, the client has no user identity, so:

Traffic from the unauthenticated Guest client → FortiAuthenticator isnot matchedby that policy.

It hits theimplicit deny, so the browser never reaches the login page.

To fix this, the administrator must:

Create or modify a firewall policy thatallows traffic from the Guest SSID subnet/interface to FortiAuthenticator and WindowsAD without requiring user authentication.

That is exactly what optionDdescribes.

Why the others are wrong:

A . Change SSID security mode to WPA2-Enterprise– External captive portals are normally used withopenSSIDs; WPA2-Enterprise uses 802.1X, not captive portal.

B . Disable HTTPS redirection– Redirection is required so users are sent to the portal; disabling it doesn't solve reachability.

C . Exclude FortiAuthenticator and Windows AD from filtering– They're already listed asexempt destinationsin the SSID configuration; the missing piece is thefirewall policy, not the exemption.

Question: 28

A network administrator connects a new FortiGate to the network, allowing it to automatically discover andI register with FortiManager.

What occurs after FortiGate retrieves the FortiManager address?

A. FortiGate establishes a secure tunnel to FortiManager over TCP port 541.

B. The device needs to be manually authorized on FortiManager.

C. FortiGate configures its interface settings based on a DHCP response from FortiManager.

D. FortiGate sends a discovery request to all devices on the local network using UDP port 1068.

Answer: A

Explanation:

When a FortiGate is deployed usingZero Touch Provisioning (ZTP)or auto-discovery:

FortiGate retrieves theFortiManager IP address(from DHCP Option 240, FortiCloud/ZTNA provisioning, or manual set).

The next step isnot UI authorizationor DHCP changes—it immediately attempts to form aFGFM (FortiGate–FortiManager) tunnel.

The FGFM protocol usesTCP port 541to establish a secure management channel.

FortiManager will still require manual authorization of the deviceinside FortiManager, but this occursafterthe tunnel is established.

Therefore, the first automatic action after retrieving the FMG address iscreating the secure FGFM tunnel on TCP/541.

Question: 29

You are setting up a captive portal to provide Wi-Fi access for visitors. To simplify the process, your team wants visitors to authenticate using their existing social media accounts instead of creating new

accounts or entering credentials manually.

Which two actions are required to enable this functionality? (Choose two.)

A. Set up a remote open authorization (OAuth) server for each selected social media platform.

B. Configure only the email login option because a social media login cannot be used with captive portals.

C. Enable Account Login as the authentication type and configure a remote LDAP server.

D. Set up the FortiAuthenticator internal database as the primary source for user credentials

E. Configure the social login profiles for the supported platforms.

Answer: A,D

Explanation:

Question: 30

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

Explanation:

When FortiAPs connect to FortiGate overIPsec tunnels, this is treated similarly to WAN/MPLS deployments.

In these scenarios, FortiGate must know that CAPWAP must traverse anon-L2transport.

FortiAP profiles include:

set mpls-connection enable

This setting is required so that:

FortiGate can encapsulate CAPWAP inside the transport tunnel

Remote FortiAPs can establish CAPWAP even when behind routed/IPsec networks

Without this option, the FortiGate detects the AP butcannot bring CAPWAP UP, leaving the AP in "discovered/unauthorized" or "ofline" state.

Why others are wrong

A . Static route→ Discovery already succeeds, so routing is not the issue.

C . Reduce MTU→ Sometimes useful for IPsec, but not required for CAPWAP establishment.

D . Firmware upgrade→ Firmware mismatch would show "Managed (upgrade required)," not CAPWAP tunnel failure.

Therefore,set mpls-connection enableis the required fix.

Question: 31

Your office wants to set up a Wi-Fi network for visitors. Your company would like to require them to log in for (racking purposes. Which two types of captive portals could be enabled on an interface? (Choose two.)

A. Terms Acknowledgment Without Authentication

B. Email Notification Only

C. Disclaimer + Authentication

D. Guest Pass Access

E. Authentication

Answer: A,E

Explanation:

A FortiGate interface can operate with different types of captive portal modes.

The available portal types that require user interaction or login include:

✓ A. Terms Acknowledgment Without Authentication

Forces users to accept terms before accessing the network

No credentials required

Still considered a captive portalCommon in guest Wi-Fi.

✓ E. Authentication

Requires username/password

Supports local users, RADIUS, LDAP, OAuth, etc.

Why the other options are incorrect

B. Email Notification Only

Not a valid captive portal mode on FortiGate.

C. Disclaimer + Authentication

This is not a selectable mode; disclaimers are part of the captive portal customization but not a standalone option.

D. Guest Pass Access

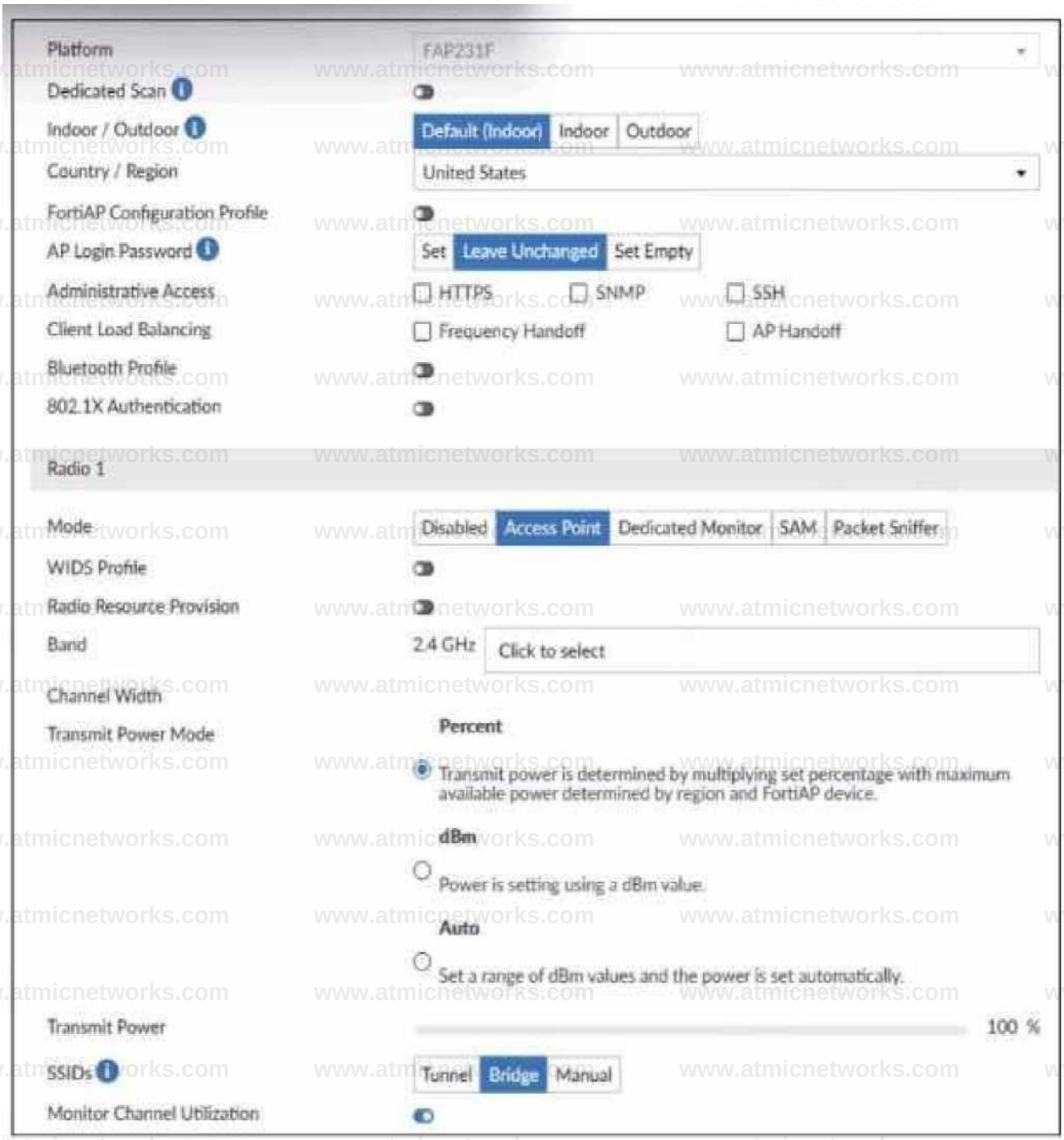
Guest pass authentication exists onFortiAuthenticator, not as a direct portal type on FortiGate.

Question: 32

Refer to the exhibits.

SSID Profiles

□ SSIDSW			
Company Printers	Guest'01	Tunnel	WPA2 Persona
Employees Red	StudentOl	Local Bridge	WPA2 Enterprise
Guest-CorpPort	fomnet	Tunnel	WPA2 Persona
PSK	fortinet	Tunnel	WPA2 Persona



A set of SSID profiles has been configured on FortiManager, and an AP profile has been assigned to a group of AP managed by FortiGate. However, none of the designated SSIDs are being broadcast by these APs.

Which configuration change is required to make the APs broadcast these SSIDs as intended?

A. Adjust the AP profile to ensure all SSIDs are configured in a supported mode, either bridge or tunnel, but not a mix of both.

B. Change the AP profile to use a platform that supports the configured mix of SSIDs.

C. Choose Manual in the SSIDs setting and select the SSIDs to broadcast.

D. Set the Transmit Power Mode to Auto.

Answer: C

Explanation:

From the exhibits:

The AP profile shows:

SSIDs: Tunnel | Bridge | Manual

The current setting isBridge, not Manual.

WhenBridgeorTunnelis selected, the AP profiledoes NOT automatically broadcast SSIDsunless the corresponding VAPs were explicitly mapped in the AP profile.

FortiManager SSID profiles are created, but unless these are explicitly applied underManual SSIDs selection, the AP will not broadcast any SSID.

Fortinet documentation states:

"To control which SSIDs an AP broadcasts, the AP Profile must have SSIDs set toManual, and the desired SSIDs must be selected."

Therefore, to make the AP broadcast the intended SSIDs:

✓You must switch the SSIDs setting to Manual, and manually select the SSIDs (CompanyPrinters, Student01, Guest-CorpPort, PSK).

Why the other options are incorrect:

A . Adjust AP profile to avoid mixing bridge/tunnelMixed modes ARE supported. Not the issue.

B . Change platformThe platform (FAP231F) already supports all listed SSIDs.

D . Set transmit power mode to autoPower settings have nothing to do with SSID broadcasting.

Question: 33

You are deploying a FortiSwitch device managed by FortiGate in a secure network environment. To ensure accurate communication, you must identify which protocols are required for communication and control between FortiGate and FortiSwitch.

Which three protocols are used by FortiGate to manage and control FortiSwitch devices? (Choose three.)

A. SNMP can be used by FortiGate to manage FortiSwitch devices by monitoring their status.

B. UHTTPS is usea;by FortiGate to securely manage and configure FortiSwitch devices.

C. FortiGate uses the Fortilink protocol to establish communication with FortiSwitch.

D. CAPWAP is used to establish the control channel between FortiSwitch and FortiGate.

E. IGMP is required for managing communication between FortiGate and FortiSwitch devices in multicast environments.

Answer: B,C,D

Explanation:

Let's verify each protocol:

C . FortiGate uses the FortiLink protocol to establish communication with FortiSwitch. ✓

FortiLink is themanagement and control protocol, encapsulated over:

LLDPfor discovery

CAPWAP (UDP/5246–5247)for control channel

DHB (Device Handshake Bus)inside CAPWAP frames

Thus,FortiLink is required.

D . CAPWAP is used to establish the control channel between FortiSwitch and FortiGate.✓

Although CAPWAP is commonly associated with FortiAP, FortiSwitchalso uses CAPWAPinternally when managed by FortiGate.

This is documented in:

FortiSwitch Administration Guide

LAN Edge deployment guide

SoD is correct.

B . UHTTPS is used by FortiGate to securely manage and configure FortiSwitch devices. ✓

FortiLink session actually uses:

Encrypted CAPWAP (over DTLS)

UHTTPS (port 4433)for secure configuration exchanges

This protocol is mandatory for:

Switch configuration synchronization

Firmware upgrade

NAC data exchange

VLAN provisioning

ThereforeUHTTPS is indeed one of the key protocols.

Why the incorrect options are wrong:

A. SNMP can be used by FortiGate to manage FortiSwitch. **X**

FortiGate doesnotuse SNMP to manage FortiSwitch.

SNMP is for monitoring by external systems, not for FortiLink control.

E . IGMP is required for management. X

IGMP is a multicast protocol, irrelevant for FortiGate–FortiSwitch management.

Question: 34

Refer to the exhibits.

FortlSwltch status

NameS	Switch Group 5	Status ▼	Model»
□ X FortlSwltch		O Offline	FortiSwitch224EPO

Fortilink interface settings in FortiGate

FortiGate (fortilink) ♦ show contig system interface edit "fortilink" set vdc-m 'rrot" met rortilmk enable set ip 10 0.2J.3 5i 355^35.2 55,0 set a 11owacceas ping tattle set type aggregate set pester "pcztV'Q set device-identification enable set ±ldp-re :ep ti :-n enable set Hdp-transmiMiM enable set role lan set s:w-ihdex 11 set auto-auth■extension device enable set xp-managed-by-tort lipas. diastole set switdi-nuncroller-nac "fortilink" set switcfc-cont roller-dynamic "forcilink* aet swc-first-create 255 set lacp-tude static next end

DHCP server setting for fortllink

corEig SyJCex liter server edit. 1
sab ins-service cteftult see nep-service local s^t defaujt-gatev>y 1 • < J, 12.254 sec netciak 25S.2SS.2S&.0 sec interrsce "foreMini" cpafig ip-;iiri5t e in 1 sec «arr-ip 10.0.13.1 set efid-ip 10.0.13.253 nexr
end
5*7 Tei-rarer, enit!?
ser mi-ary un; "F re J £K render[R] next.

end

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

Which misconfiguration might be preventing FortiGate from detecting FortiSwitch?

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 staysOfline.

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.

Question: 35

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

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: 36

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

Explanation:

WithAD machine authenticationvia FortiAuthenticator:

When a machine successfully authenticates, FortiAuthenticator records:

Machine account / identity

MAC addressof the device

Associated IP and session info

To handle sleep/hibernation:

FortiAuthenticator keeps acache of authenticated MAC addressesfor a configured timeout.

When the device wakes up and sends traffic again, FortiAuthenticator/FSSO can still treat it as authenticated as long as its MAC is in cache, so access is maintained without forcing a full machine re-auth immediately.

This matches optionD.

A(guest VLAN) is not the standard behavior here.

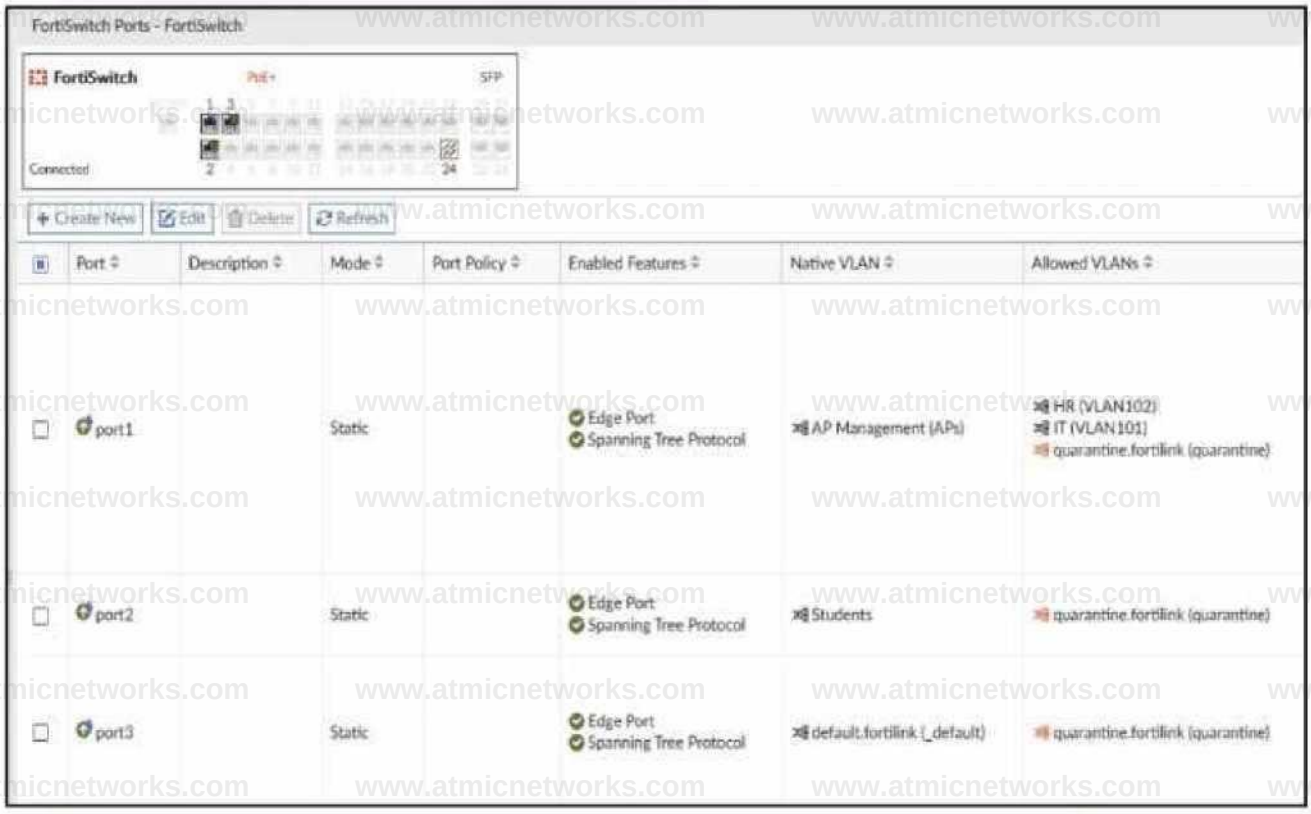
B(WoL) is unrelated.

C(IP-based) would break as IPs can change; MAC-based caching is what's used.

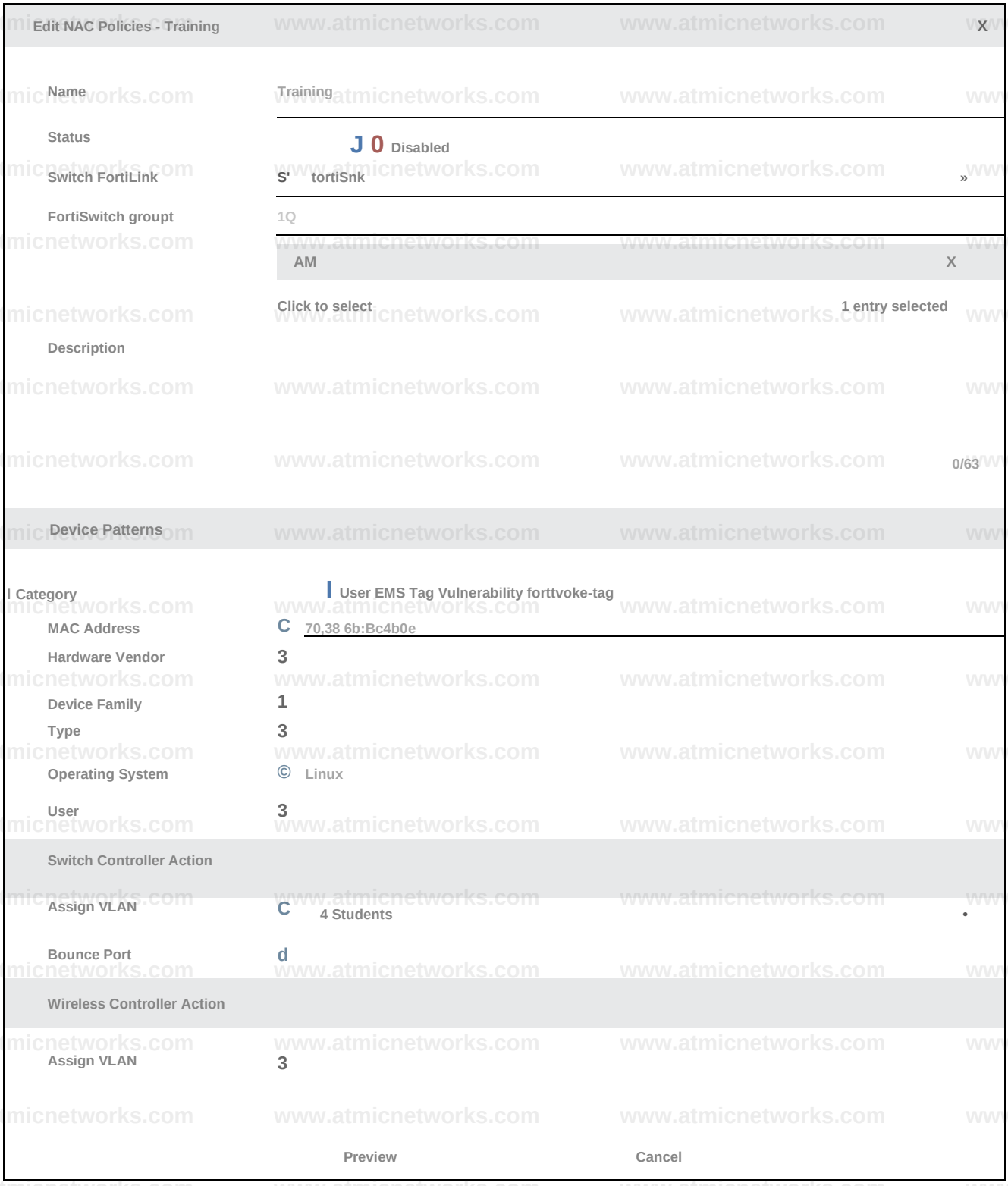
Question: 37

Refer to the exhibits.

FortiSwitch Ports



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

Explanation:

From the exhibits:

FortiSwitch Ports viewshows:

port2

Mode: Static

Native VLAN: Students

Allowed VLANs: quarantine.fortilink (quarantine)

NAC policy “Training”:

Switch FortiLink: fortilink

Category:Device

Matching criteria:

MAC Address: 70:88:6b:8c:4b:0e (enabled)

Operating System:Linux(enabled)

Switch Controller Action:

Assign VLAN = Students

Bounce Port = enabled

Design intent:

Device with that MAC + OS Linux, when plugged intoport2, should be dynamically moved to VLANStudentsby the NAC policy.

Why it doesn’t work now

On FortiLink NAC,dynamic NAC decisions only apply on ports whose “Access Mode” is set to NAC:

NAC mode = FortiGate controls theonboarding VLAN, evaluates NAC policies, and then dynamically reassigns the switch port VLAN (access, quarantine, etc.).

Static mode(what we see on port2) means the port just uses its configurednative/allowed VLANs, andno NAC classificationhappens.

Right now:

port2 is astatic access portwith Native VLAN = Students.

The NAC policy exists, butFortiSwitch is not in NAC enforcement mode on that port, so the policy is never evaluated for traffic on port2.

Therefore, themissing configurationis:

Setport2toNAC mode(sometimes called “Access mode: NAC” or “NAC LAN edge port”).

Once port2 is changed to NAC mode:

Device initially lands in the onboarding/quarantine VLAN.

FortiGate collects device info (MAC, OS, etc.).

NAC policy “Training” matches MAC + Linux.

Switch controller actionAssign VLAN = Studentsis applied.

Port is bounced (if configured), bringing the device back up in VLAN Students.

Why the other options are wrong

B . MAC or OS misconfigured

Possible in general, but the question asks forwhich configuration is missing, and the exhibits clearly focus on port mode. Also, even with wrong MAC/OS, the port would still be in NAC mode; here NAC isn’t even active.

C . Port Policy mode

Port policy (edge/trunk) is separate from NAC; NAC requires the specificNAC access mode.

D . Students VLAN should be Allowed VLANs instead of Native VLAN

For an access port, having Students as thenative VLANis correct. NAC policy’s Assign VLAN will set that as access VLAN; no need to make it an allowed trunk VLAN.

Question: 38

You are troubleshooting a Syslog-based single sign-on (SSO) issue on FortiAuthenticator, where user authentication is not being correctly mapped from the syslog messages. You need a tool to diagnose the issue and understand the logs to resolve it quickly.

Which tool in FortiAuthenticator can you use to troubleshoot and diagnose a Syslog SSO issue?

A. Debug logs > Remote Servers > Syslog Viewer

B. Parsing Test Tool

C. Debug logs > SSO Sessions page

D. Debug logs > Single Sign-On > Syslog SSO

Answer: D

Explanation:

Context: You're troubleshootingSyslog-based SSOonFortiAuthenticator:

Devices (typically firewalls, WLAN controllers, VPN gateways) sendsyslog messagescontaining usernames, IPs, login/logout events.

FortiAuthenticator parses those logs usingSyslog SSO rulesand injects logon sessions intoFSSOfor FortiGate.

When users are not mapping correctly, you need to see:

Did the syslog message arrive?

Which matching rule (if any) caught it?

What username and IP were extracted?

Why was a message ignored or rejected?

FortiAuthenticator has a dedicated debug area for this:

Debug logs → Single Sign-On → Syslog SSO

This view shows:

Raw syslog lines received

Thematching ruleapplied (or "no match")

Parsed fields (username, IP, group)

Any parsing errors

This is exactly the tool designed totroubleshoot and diagnose Syslog SSO issues.

Why the other options are not the best for this issue

A . Debug logs > Remote Servers > Syslog Viewer

Lets you see syslog traffic in general, but doesnotshow how SSO rules are applied or why they fail. Good for connectivity checks, not SSO logic.

B . Parsing Test Tool

Useful totestpatterns and rules manually by pasting sample log lines, but it doesn't show live traffic or running SSO sessions.

C . Debug logs > SSO Sessions page

Shows existing SSO sessions (who is logged in), but notwhya particular syslog message did not create a session.

Question: 39

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

Explanation:

Observed behavior:

Devices in the VLANcan ping FortiGate→ gateway reachability OK.

FortiGatecan ping devicesin that VLAN → return path OK.

Inter-VLAN routingworks → FortiGate's L3 and policies are fine.

Devices in the same VLAN cannot ping each other→ problem is on theL2 switching plane, not L3.

On FortiSwitch (managed by FortiGate), there is a feature calledAccess VLAN(sometimes described in NAC/dynamic

segmentation context):

WhenAccess VLANis enabled on a VLAN, the switchdoes not perform normal L2 forwardingbetween hosts in that VLAN.

Instead, all traffic from endpoints in that VLAN isforced upstream to FortiGate, as if every frame were destined for the gateway.

This is used for designs where you wantall intra-VLAN traffic inspected by the firewall, implementing micro-segmentation.

Resulting behavior:

Host → FortiGate: works (frames are forwarded to FortiGate).

FortiGate → Host: works (routed back).

Host A → Host B (same VLAN):

Frame from A goes to FortiGate.

FortiGate seessource and destination in same subnet; depending on policy, it may drop or not have a policy allowing that traffic.

Even if allowed, certain designs still break pure L2 expectations.

In the exam scenario, the key point is:

IfAccess VLAN is enabled,local L2 communication within that VLAN is disabled, so hosts in the same VLAN cannot communicate directly.

That perfectly explains:

Same VLAN hosts can’t ping each other

But they can both reach FortiGate and beyond

Why the other options are less likely / incorrect

B . FortiSwitch MAC address table is missing entries

If MAC table were empty/bad,nothingin that VLAN would work properly, including pinging FortiGate.

C . FortiGate ARP table is missing entries

Then FortiGate couldn’t ping the devices either; but it can.

D . Native VLAN misconfigured on ports

That would affect connectivity to FortiGate too, not only host-to-host.

Question: 40

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

Explanation:

In FortiGate captive portal workflows (local or external):

Client connects to SSID / interface that has captive portal enabled.

Client makes an HTTP/HTTPS request.

FortiGate intercepts and redirects to alogin page(local or external URL).

The portal form is submitted viaPOSTback to FortiGate.

To prevent tampering and to tie the POST back to thecorrect user session, FortiGate includes a special hidden parameter in the redirect and expects it in the POST:

The parameter is namedmagic.

The magic value:

Is aunique tokengenerated per captive-portal session.

Encodes/session-links the user's IP, interface, and session info.

Allows FortiGate to ensure that:

The POST comes from the user who initiated the original request.

The request is not a random or replayed submission.

When troubleshooting:

If the external portal does notpreserve and resendthe magic parameter back to FortiGate exactly as received,

authentication fails, and you'll see errors like "session not found" or "invalid magic".

Why the other fields are not used for this purpose

A . username– Just the login ID; multiple users can use the same username from different locations, so it can't uniquely track the browser session.

B . redir– Contains the URL the user originally requested, so they can be sent back there after login. It is not a session integrity token.

D . email– Optional field used in some guest/registration flows; irrelevant to session validation.