



Fortinet

Exam Questions FCSS_LED_AR-7.6

FCSS - LAN Edge 7.6 Architect

About ExamBible

Your Partner of IT Exam

Found in 1998

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

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

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

NEW QUESTION 1

Refer to the exhibit.

WTP profile configuration

```

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

```

Which shows the WTP profile configuration.

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

A dual-band-capable client enters the area near the first AP and the first AP measures the new client at -33 dBm signal strength. The second AP measures the new client at -43 dBm signal strength.

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

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

Answer: C

NEW QUESTION 2

Refer to the exhibits.

SSID Profiles

| SSIDs (4) | | | | |
|--------------------------|-----------------|-----------|--------------|-----------------|
| <input type="checkbox"/> | CompanyPrinters | Guest-01 | Tunnel | WPA2 Personal |
| <input type="checkbox"/> | Employees-Red | Student01 | Local Bridge | WPA2 Enterprise |
| <input type="checkbox"/> | Guest-CorpPort | fortinet | Tunnel | WPA2 Personal |
| <input type="checkbox"/> | PSK | fortinet | Tunnel | WPA2 Personal |

Platform: FAP231F

Dedicated Scan:

Indoor / Outdoor: **Default (Indoor)** Indoor Outdoor

Country / Region: United States

FortiAP Configuration Profile:

AP Login Password: **Set** Leave Unchanged Set Empty

Administrative Access: HTTPS SNMP SSH

Client Load Balancing: Frequency Handoff AP Handoff

Bluetooth Profile:

802.1X Authentication:

Radio 1

Mode: **Access Point** Disabled Dedicated Monitor SAM Packet Sniffer

WIDS Profile:

Radio Resource Provision:

Band: 2.4 GHz

Channel Width:

Transmit Power Mode: **Percent**

Transmit power is determined by multiplying set percentage with maximum available power determined by region and FortiAP device.

dBm
Power is setting using a dBm value.

Auto
Set a range of dBm values and the power is set automatically.

Transmit Power: 100 %

SSIDs: **Tunnel** Bridge Manual

Monitor Channel Utilization:

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

NEW QUESTION 3

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

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

Answer: D

NEW QUESTION 4

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

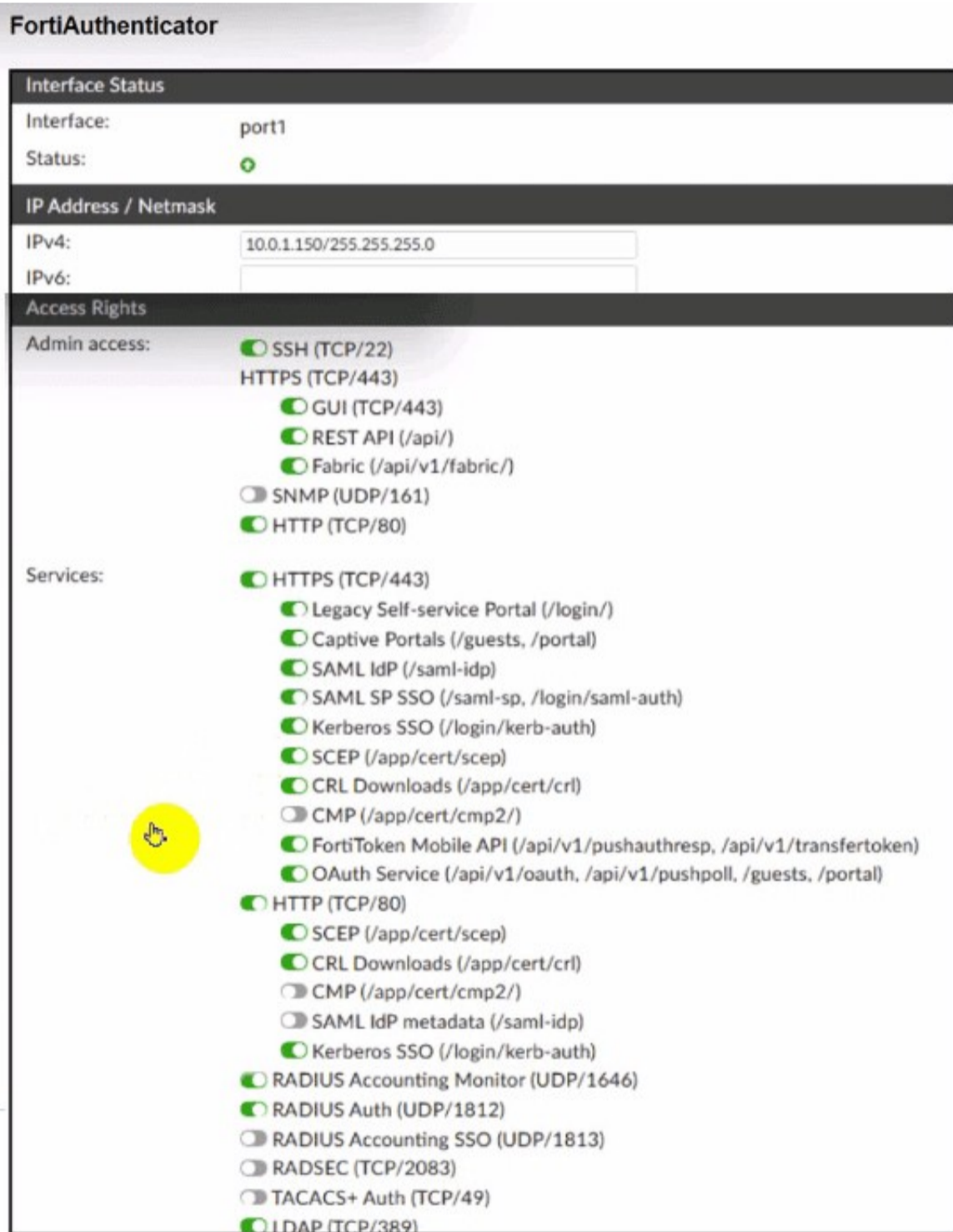
- A. Ensure that the FortiGate security policies allow traffic from the FortiSwitch.
- B. Manually assign a static IP to the FortiSwitch.
- C. Verify that FortiGate device DHCP server is assigning an IP to the FortiSwitch.
- D. Ensure the FortiSwitch has internet access.

Answer: C

NEW QUESTION 5

Refer to the exhibits.

FortiAuthenticator

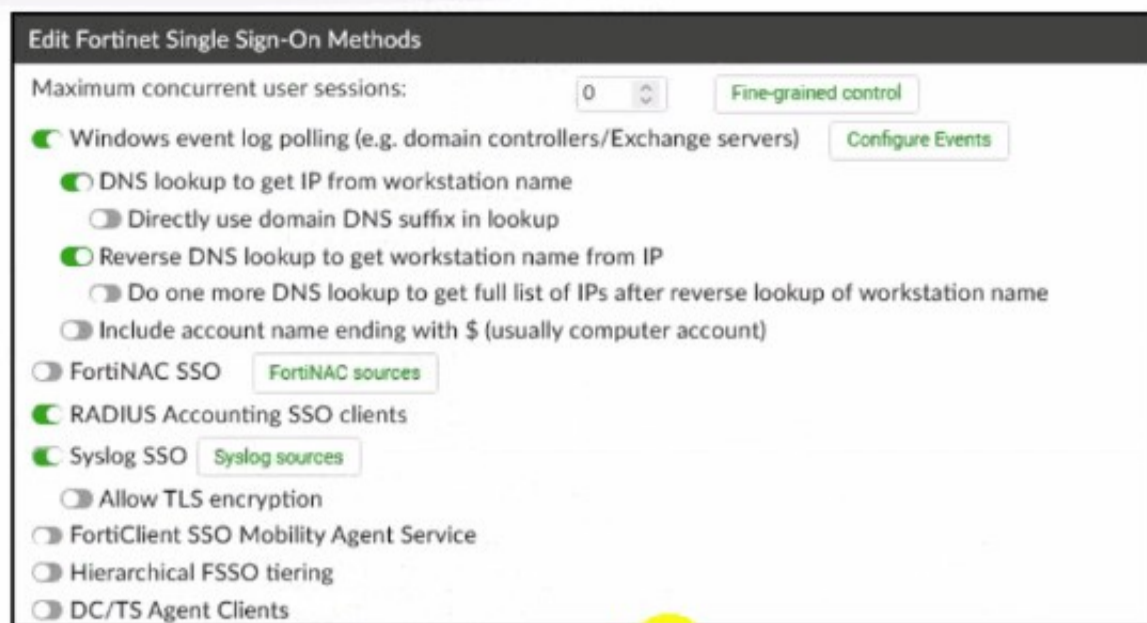


The screenshot shows the FortiAuthenticator configuration interface. It is divided into three main sections:

- Interface Status:** Shows 'Interface: port1' and 'Status: [green up arrow]'.
- IP Address / Netmask:** Shows 'IPv4: 10.0.1.150/255.255.255.0' and 'IPv6: [empty]'.
- Access Rights:**
 - Admin access:** Includes SSH (TCP/22), HTTPS (TCP/443) with sub-options GUI (TCP/443), REST API (/api/), and Fabric (/api/v1/fabric/); SNMP (UDP/161); and HTTP (TCP/80).
 - Services:** Includes HTTPS (TCP/443) with various portals and SSO options; HTTP (TCP/80) with SCEP, CRL Downloads, CMP, SAML IdP metadata, and Kerberos SSO; RADIUS Accounting Monitor (UDP/1646), RADIUS Auth (UDP/1812), RADIUS Accounting SSO (UDP/1813), RADSEC (TCP/2083), TACACS+ Auth (TCP/49), and LDAP (TCP/389).

A yellow circle highlights the 'HTTP (TCP/80)' option under the 'Services' section.

FortiAuthenticator SSO Methods



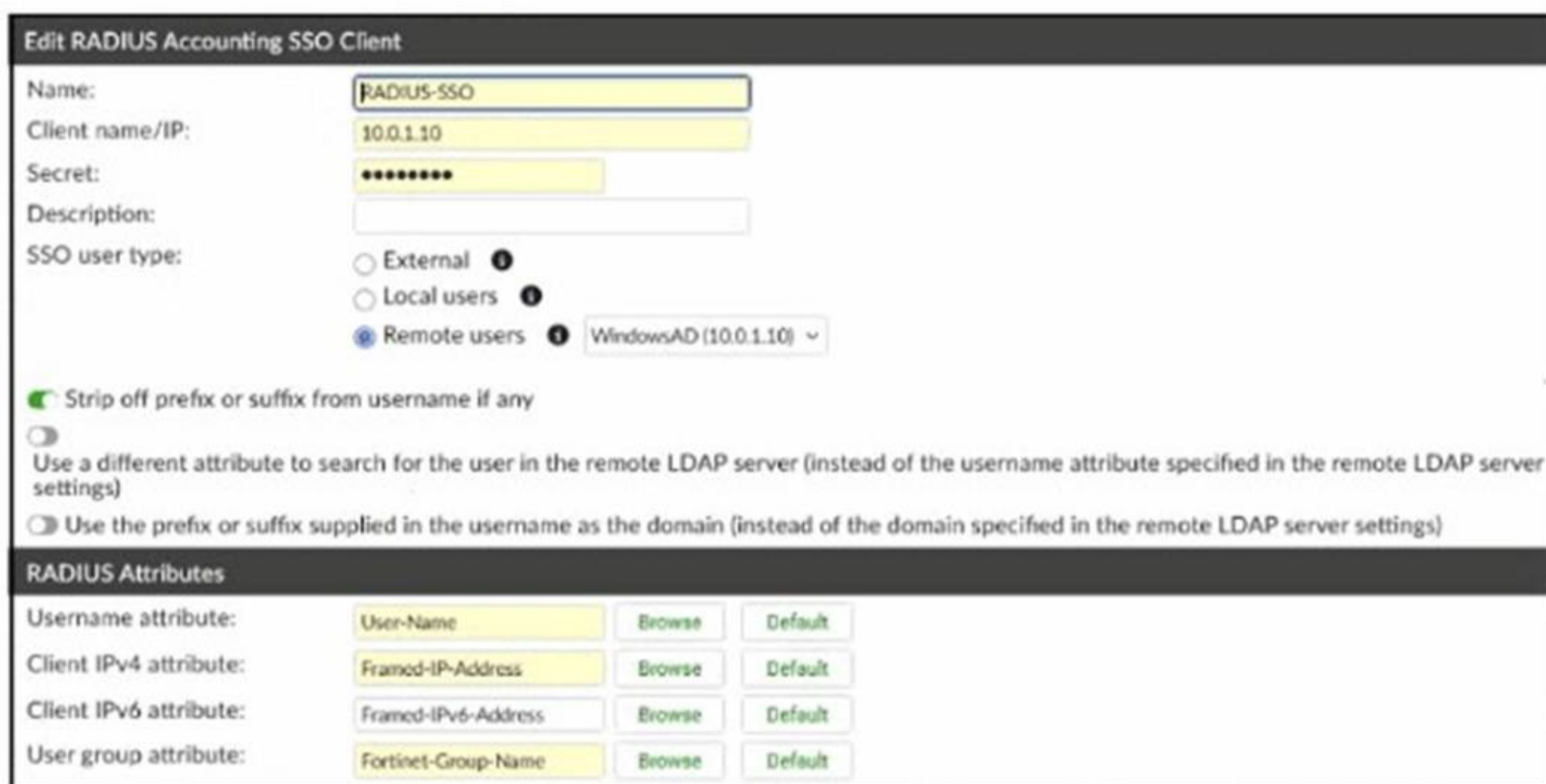
Edit Fortinet Single Sign-On Methods

Maximum concurrent user sessions: Fine-grained control

Windows event log polling (e.g. domain controllers/Exchange servers) Configure Events

- DNS lookup to get IP from workstation name
 - Directly use domain DNS suffix in lookup
- Reverse DNS lookup to get workstation name from IP
 - Do one more DNS lookup to get full list of IPs after reverse lookup of workstation name
 - Include account name ending with \$ (usually computer account)
- FortiNAC SSO FortiNAC sources
- RADIUS Accounting SSO clients
- Syslog SSO Syslog sources
 - Allow TLS encryption
- FortiClient SSO Mobility Agent Service
- Hierarchical FSSO tiering
- DC/TS Agent Clients

FortiAuthenticator RADIUS Accounting SS Client



Edit RADIUS Accounting SSO Client

Name:

Client name/IP:

Secret:

Description:

SSO user type:

- External ⓘ
- Local users ⓘ
- Remote users ⓘ

Strip off prefix or suffix from username if any

Use a different attribute to search for the user in the remote LDAP server (instead of the username attribute specified in the remote LDAP server settings)

Use the prefix or suffix supplied in the username as the domain (instead of the domain specified in the remote LDAP server settings)

RADIUS Attributes

| | | | |
|------------------------|--|---------------------------------------|--|
| Username attribute: | <input type="text" value="User-Name"/> | <input type="button" value="Browse"/> | <input type="button" value="Default"/> |
| Client IPv4 attribute: | <input type="text" value="Framed-IP-Address"/> | <input type="button" value="Browse"/> | <input type="button" value="Default"/> |
| Client IPv6 attribute: | <input type="text" value="Framed-IPv6-Address"/> | <input type="button" value="Browse"/> | <input type="button" value="Default"/> |
| User group attribute: | <input type="text" value="Fortinet-Group-Name"/> | <input type="button" value="Browse"/> | <input type="button" value="Default"/> |

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

NEW QUESTION 6
 Refer to the exhibits.

FortiGate Security Fabric widget

The screenshot shows a 'Core Network Security' dashboard with two main widgets. The left widget, 'Security Fabric Setup', has a red background and includes a 'Training' input field. The right widget, 'FortiAnalyzer Logging', has a blue background, a refresh icon, and displays the IP address '10.0.1.210' with a green plus icon.

Security Fabric Automation Stitch

The 'Edit Automation Stitch' page shows the following configuration:

- Name:** IOC
- Status:** Enable (selected), Disable
- FortiGate(s):** All FortiGates
- Action execution:** Sequential (selected), Parallel
- Description:** (empty text field, 0/255 characters)

The 'Stitch' section displays a workflow diagram:

- Trigger:** Compromised Host - High
- Action:** Quarantine on FortiSwitch + FortiAP
- Buttons:** Add delay, Add Action

Quarantine widget



FortiGate firewall policy

| Name | Source | Destination | Schedule | Service | Action | NAT | Security Profiles | Log |
|------------------|----------|-------------|----------|---------|--------|--------|-------------------|---------------------------------|
| Students → port1 | Internet | all | all | always | ALL | ACCEPT | Enabled | default, certificate-inspection |
| Implicit | | | | | | | | |

FortiAnalyzer log

| # | Date/Time | Device ID | User | Source | Destination IP | Service | Host Name | Action | URL | Category | Description |
|---|-----------|-----------------|------|----------|----------------|---------|-----------|---------|------------------------------|--------------------|-------------|
| 1 | 11:16:29 | FGVM1V000014... | | 10.0.2.2 | 23.217.138.108 | HTTP | abcomm.nl | blocked | http://abcomm.nl/ | Malicious Websites | |
| 2 | 11:16:29 | FGVM1V000014... | | 10.0.2.2 | 23.217.138.108 | HTTP | abcomm.nl | blocked | http://abcomm.nl/favicon.ico | Malicious Websites | |

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: CD

NEW QUESTION 7

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

- A. It makes the certificate easier to revoke manually because it reduces the need for automatic checks.
- B. It limits the validity of the certificate to specific devices and applications, reducing its general usability.
- C. It enables precise identification of the user and ensures timely certificate revocation checks.
- D. It makes the certificate compatible with a wide range of applications and services by ensuring universal validity

Answer: C

NEW QUESTION 8

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

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

Answer: C

NEW QUESTION 9

Refer to the exhibits.

FortiGate RSSO configuration

Edit External Connector

Endpoint/Identity



RADIUS Single Sign-On Agent

Connector Settings


Name

Use RADIUS Shared Secret


Send RADIUS Responses



FortiGate interface configuration



Edit Interface

Name  port3

Alias

Type  Physical Interface

VRF ID  

Role  

Address


Addressing mode Manual DHCP Auto-managed by IPAM


IP/Netmask


Secondary IP address

Administrative Access

IPv4


| | | |
|---|---|---|
| <input checked="" type="checkbox"/> HTTPS | <input checked="" type="checkbox"/> HTTP | <input checked="" type="checkbox"/> PING |
| <input type="checkbox"/> FMG-Access | <input checked="" type="checkbox"/> SSH | <input type="checkbox"/> SNMP |
| <input type="checkbox"/> FTM | <input checked="" type="checkbox"/> RADIUS Accounting | <input type="checkbox"/> Security Fabric Connection  |
| <input type="checkbox"/> Speed Test | | |

Receive LLDP  Use VDOM Setting Enable Disable

Transmit LLDP  Use VDOM Setting Enable Disable

DHCP Server

Network

Device detection 

Security mode

Examine the FortiGate RSO configuration shown in the exhibit.

FortiGate is set up to use RSO 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 RSO user groups.

Which three critical configurations must you implement on the FortiGate device? (Choose three.)

- A. The RADIUS Attribute Value setting configured for an RSO user group should match the class RADIUS attribute value in the RADIUS accounting message.
- B. RSO 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 RSO agent configuration should be set to Class.
- E. The rso-endpoint-attribute CLI setting in the RSO agent configuration should be set to User-Name.

Answer: ADE

NEW QUESTION 10

.....

Relate Links

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

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

Contact us

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

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