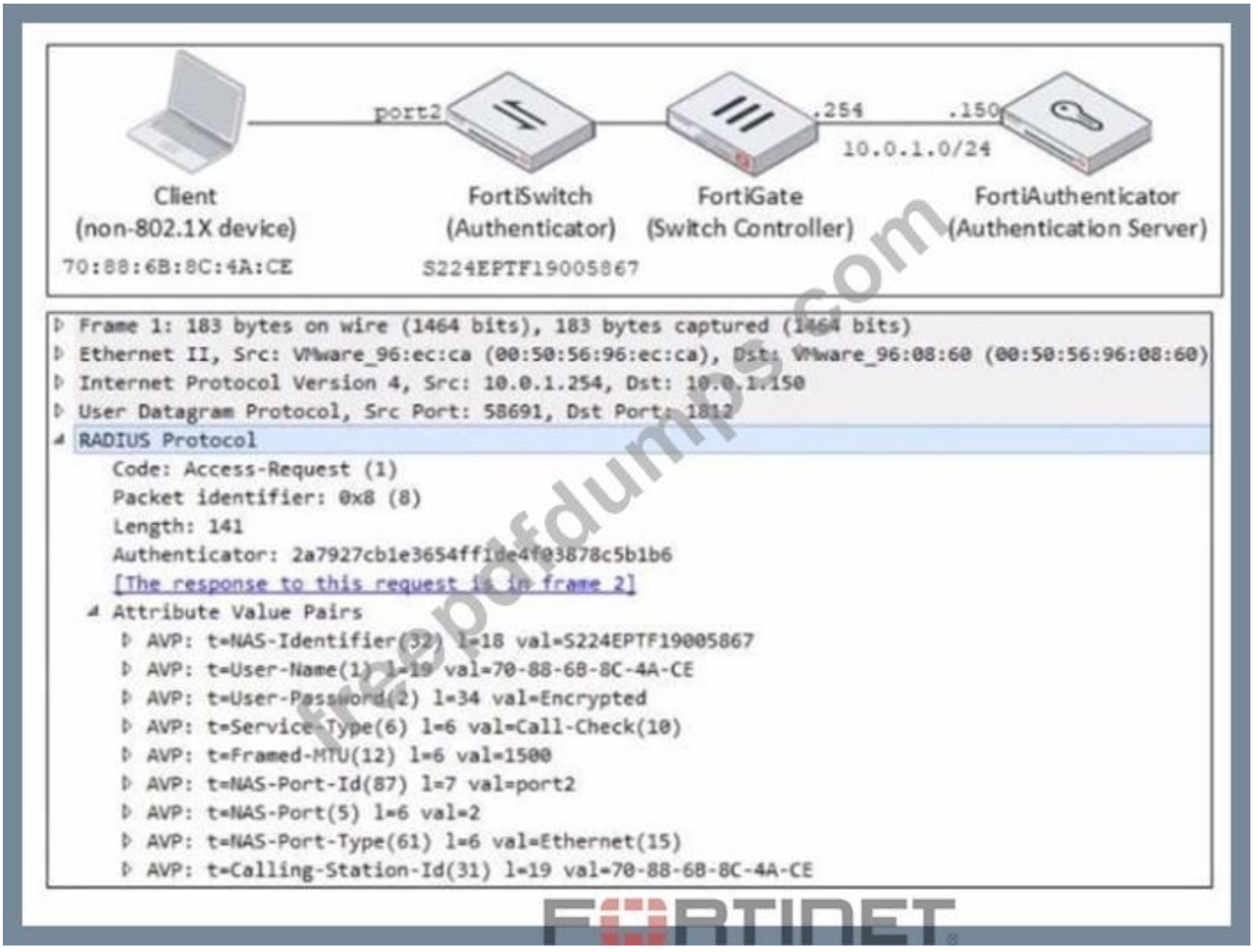
Fortinet.NSE7_LED-7.0.v2024-08-20.q13

Exam Code:	NSE7_LED-7.0
Exam Name:	Fortinet NSE 7 - LAN Edge 7.0
Certification Provider:	Fortinet
Free Question Number:	13
Version:	v2024-08-20
# of views:	791
# of Questions views:	130
https://www.freepdfdumps.com/Fortinet.NSE7_LED-7.0.v2024-08-20.q13.html	

NEW QUESTION: 1

Refer to the exhibit.



Examine the network diagram and packet capture shown in the exhibit

The packet capture was taken between FortiGate and FortiAuthenticator and shows a RADIUS Access-Request packet sent by FortiSwitch to FortiAuthenticator through FortiGate Why does the User-Name attribute in the RADIUS Access-Request packet contain the client MAC address?

A. The client is performing AD machine authentication

B. FortiSwitch is authenticating the client using MAC authentication bypass

C. The client is performing user authentication

D. FortiSwitch is sending a RADIUS accounting message to FortiAuthenticator

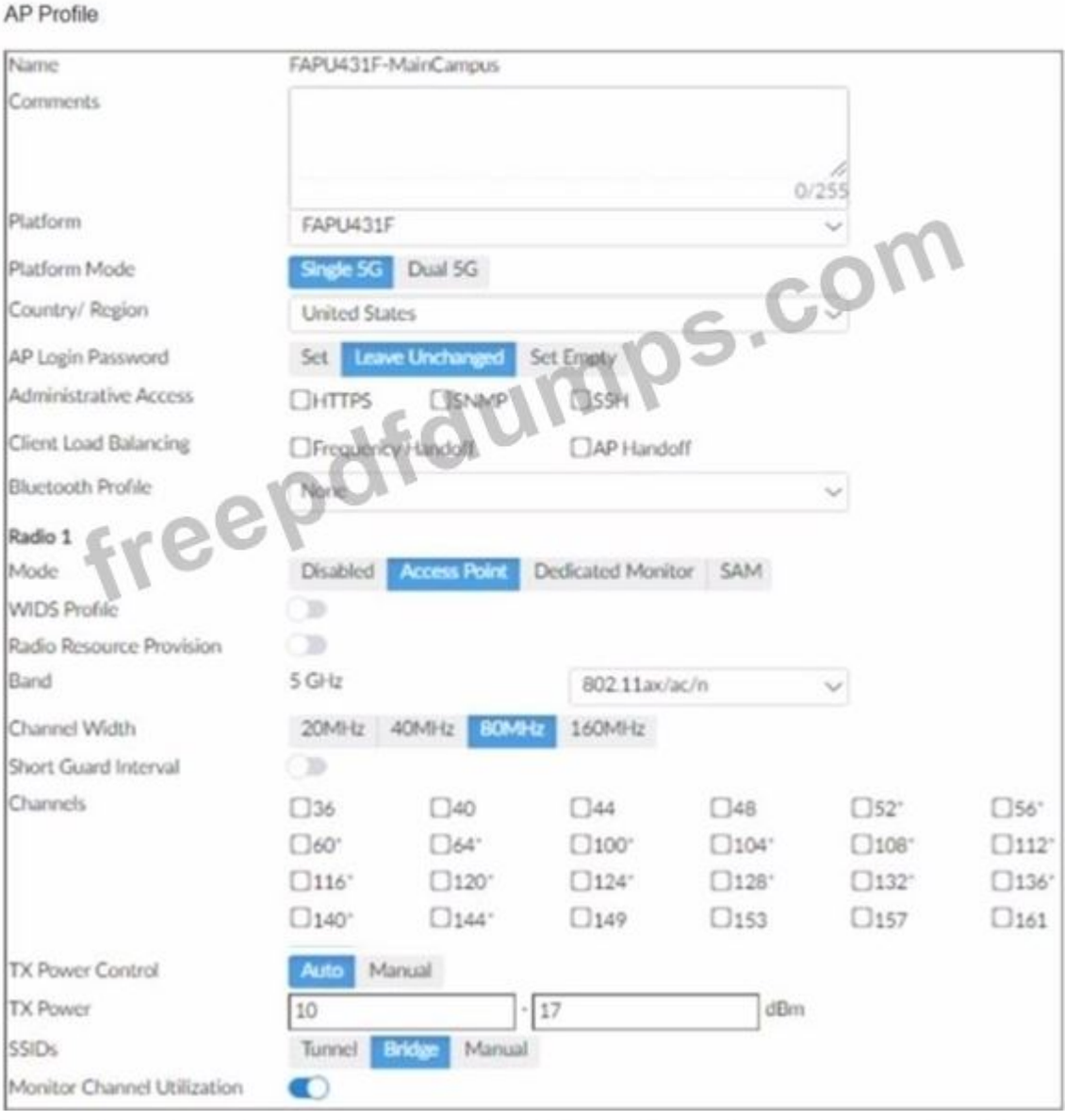
Answer: B (LEAVE A REPLY)

Explanation

According to the exhibit, the User-Name attribute in the RADIUS Access-Request packet contains the client MAC address of 00:0c:29:6a:2b:3d. This indicates that FortiSwitch is authenticating the client using MAC authentication bypass (MAB), which is a method of authenticating devices that do not support 802.1X by using their MAC address as the username and password. Therefore, option B is true because it explains why the User-Name attribute contains the client MAC address. Option A is false because AD machine authentication uses a computer account name and password, not a MAC address. Option C is false because user authentication uses a user name and password, not a MAC address. Option D is false because FortiSwitch is sending a RADIUS Access-Request message to FortiAuthenticator, not a RADIUS accounting message.

NEW QUESTION: 2

Refer to the exhibits



The exhibits show the wireless network (VAP) SSID profiles defined on FortiManager and an AP profile assigned to a group of APs that are supported by FortiGate None of the APs are broadcasting the SSIDs defined by the AP profile Which changes do you need to make to enable the SSIDs to broadcast?

A. In the SSIDs section enable Tunnel

B. Enable one channel in the Channels section

C. Enable multiple channels in the Channels section and enable Radio Resource Provision

D. In the SSIDs section enable Manual and assign the networks manually

Answer: B (LEAVE A REPLY)

Explanation
According to the FortiManager Administration Guide1, "To enable the SSID, you must select at least one channel for the radio. If no channels are selected, the SSID will not be enabled." Therefore, enabling one channel in the Channels section will allow the SSIDs to broadcast.

NEW QUESTION: 3
A wireless network in a school provides guest access using a captive portal to allow unregistered users to self-register and access the network The administrator is requested to update the existing configuration to provide captive portal authentication through a secure connection (HTTPS) Which two changes must the administrator make to enforce HTTPS authentication"? (Choose two >
A. Create a new SSID with the HTTPS captive portal URL
B. Enable HTTP redirect in the user authentication settings
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: (SHOW ANSWER)
Explanation
According to the FortiGate Administration Guide, "To enable HTTPS authentication, you must enable HTTP redirect in the user authentication settings. This redirects HTTP requests to HTTPS. You must also update the captive portal URL to use HTTPS on both FortiGate and FortiAuthenticator." Therefore, options B and D are true because they describe the changes that the administrator must make to enforce HTTPS authentication for the captive portal. Option A is false because creating a new SSID with the HTTPS captive portal URL is not required, as the existing SSID can be updated with the new URL. Option C is false because disabling HTTP administrative access on the guest SSID will not enforce HTTPS connection, but rather block HTTP connection.

NEW QUESTION: 4
You are configuring a FortiGate wireless network to support automated wireless client quarantine using IOC Which two configurations must you put in place for a wireless client to be quarantined successfully? (Choose two)
A. Configure the wireless network to be in tunnel mode
B. Configure the FortiGate device in the Security Fabric with a FortiAnalyzer device
C. Configure a firewall policy to allow communication
D. Configure the wireless network to be in bridge mode
Answer: A,B (LEAVE A REPLY)
Explanation
According to the FortiGate Administration Guide, "To enable automated wireless client quarantine using IOC, you must configure the following settings: Configure your wireless network to be in tunnel mode. This allows FortiGate to inspect all wireless traffic and applysecurity policies. Configure your FortiGate device in the Security Fabric with a FortiAnalyzer device. This allows

FortiAnalyzer to detect indicators of compromise (IOC) from wireless traffic and send quarantine commands to FortiGate." Therefore, options A and B are true because they describe the configurations that must be put in place for a wireless client to be quarantined successfully using IOC. Option C is false because configuring a firewall policy to allow communication is not required, as the default firewall policy for tunnel mode wireless networks is to allow all traffic. Option D is false because configuring the wireless network to be in bridge mode is not supported, as FortiGate cannot inspect or quarantine wireless traffic in bridge mode.

NEW QUESTION: 5

Refer to the exhibits.

```
# get wireless-controller rf-analysis
WTP: Office  0-192.168.5.98:5246
     channel    rssi-total    rf-score     overlap-ap    interfere-ap chan-utilizaion
           1            66           8             11              11             32%
           2            13          10              0              20             44%
           3             6          10              0              20             16%
           4            14          10              0              20             13%
           5            31          10              0              20             50%
           6           137           3              9               9             73%
           7            32          10              0              12             58%
           8            17          10              0              12              9%
           9            12          10              0              14              1%
          10            20          10              0              14             17%
          11            79           7              3               5             32%
          12            24          10              0               5             18%
          13            32          10              2               5             22%
```


Exhibit.

Examine the troubleshooting outputs shown in the exhibits

Users have been reporting issues with the speed of their wireless connection in a particular part of the wireless network The interface that is having issues is the 2 4 GHz interface that is currently configured on channel 6 The administrator of the wireless network has investigated and surveyed the local RF environment using the tools available at the AP and FortiGate Which configuration would improve the wireless connection?

A. Change the AP 2 4 GHz channel to 11

B. Change the AP 2 4 GHz channel to 1.

C. Change the AP 2 4 GHz channel to 9.

D. Change the AP 2 4 GHz channel to 13.

Answer: B (LEAVE A REPLY)

Explanation

According to the exhibits, the AP 2.4 GHz interface is currently configured on channel 6, which is overlapping with other nearby APs on channels 4 and 8. This can cause interference and reduce the wireless performance.

Therefore, changing the AP 2.4 GHz channel to 1 would improve the wireless connection, as it would avoid the overlapping channels and use a non-overlapping channel instead. Option A is false because changing the AP 2.4 GHz channel to 11 would still overlap with other nearby APs on channels 9 and 13. Option C is false because changing the AP 2.4 GHz channel to 9 would

still overlap with other nearby APs on channels 6, 8, and 11. Option D is false because changing the AP 2.4 GHz channel to 13 would still overlap with other nearby APs on channels 9 and 11.

NEW QUESTION: 6
An administrator has configured an SSID in bridge mode for corporate employees All APs are online and provisioned using default AP profiles Employees are unable to locate the SSID to conned Which two configurations can the administrator verify? (Choose two)
A. Verify that the broadcast SSID option is enabled in the SSID configuration
B. Verify that the Block Intra-SSID Traffic (intra-vap-privacy) option in the SSID configuration is disabled
C. Verify that the SSID to an AP group that should be broadcasting the SSID is applied
D. Verify that the SSID is manually applied on AP profiles for both 2 4 GHz and 5 GHz radios
Answer: A,C (LEAVE A REPLY)
Explanation
According to the FortiAP Configuration Guide1, "To enable the SSID, you must select at least one channel for the radio. If no channels are selected, the SSID will not be enabled. You must also enable Broadcast SSID." Therefore, option A is true because the broadcast SSID option allows the SSID to be visible to wireless clients.
Option C is also true because the SSID must be applied to an AP group that contains the APs that should be broadcasting the SSID. According to the same guide1, "You can create AP groups and assign them to different locations or departments. You can then apply different settings, such as SSIDs, to each group." Option B is false because blocking intra-SSID traffic prevents wireless clients on the same SSID from communicating with each other, which is not related to broadcasting the SSID. Option D is false because the SSID can be applied to an AP group or a global profile, which will automatically apply to all APs, without manually configuring each AP profile.

NEW QUESTION: 7
Which CLI command should an administrator use to view the certificate verification process in real time?
A. diagnose debug application foauthd -1
B. diagnose debug application radiusd -1
C. diagnose debug application authd -1
D. diagnose debug application fnbamd -1
Answer: A (LEAVE A REPLY)
Explanation
According to the FortiOS CLI Reference Guide, "The diagnose debug application foauthd command enables debugging of certificate verification process in real time." Therefore, option A is true because it describes the CLI command that an administrator should use to view the certificate verification process in real time. Option B is false because diagnose debug application radiusd -1 enables debugging of RADIUS authentication process, not certificate verification

process. Option C is false because diagnose debug application authd -1 enables debugging of authentication daemon process, not certificate verification process. Option D is false because diagnose debug application fnbamd -1 enables debugging of FSSO daemon process, not certificate verification process.

NEW QUESTION: 8
You are investigating a report of poor wireless performance in a network that you manage. The issue is related to an AP interface in the 5 GHz range You are monitoring the channel utilization over time.
What is the recommended maximum utilization value that an interface should not exceed?
A. 85%
B. 95%
C. 75%
D. 65%
Answer: D (LEAVE A REPLY)
Explanation
According to the FortiAP Configuration Guide, "Channel utilization measures how busy a channel is over a given period of time. It includes both Wi-Fi and non-Wi-Fi interference sources. A high channel utilization indicates a congested channel and can result in poor wireless performance. The recommended maximum utilization value that an interface should not exceed is 65%."
Therefore, option D is true because it gives the recommended maximum utilization value for an interface in the 5 GHz range. Options A, B, and C are false because they give higher utilization values that can cause poor wireless performance.
https://docs.fortinet.com/document/fortiap/7.0.0/configuration-guide/734537/wireless-radio-settings#channel-uti

NEW QUESTION: 9
Refer to the exhibit.
Examine the FortiGate configuration FortiAnalyzer logs and FortiGate widget shown in the exhibit An administrator is testing the Security Fabric quarantine automation The administrator added FortiAnalyzer to the Security Fabric and configured an automation stitch to automatically quarantine compromised devices The test device (::.:.:.!) s connected to a managed Fort Switch dev :e After trying to access a malicious website from the test device, the administrator verifies that FortiAnalyzer has a log (or the test connection However the device is not getting quarantined by FortiGate as shown in the quarantine widget Which two scenarios are likely to cause this issue? (Choose two)
A. The web filtering rating service is not working
B. FortiAnalyzer does not have a valid threat detection services license
C. The device does not have FortiClient installed
D. FortiAnalyzer does not consider the malicious website an indicator of compromise (IOC)
Answer: (SHOW ANSWER)

Explanation
According to the exhibits, the administrator has configured an automation stitch to automatically quarantine compromised devices based on FortiAnalyzer's threat detection services. However, according to the FortiAnalyzer logs, the test device is not detected as compromised by FortiAnalyzer, even though it tried to access a malicious website. Therefore, option B is true because FortiAnalyzer does not have a valid threat detection services license, which is required to enable the threat detection services feature. Option D is also true because FortiAnalyzer does not consider the malicious website an indicator of compromise (IOC), which is a criterion for identifying compromised devices. Option A is false because the web filtering rating service is working, as shown by the log entry that indicates that the test device accessed a URL with a category of
"Malicious Websites". Option C is false because the device does not need to have FortiClient installed to be quarantined by FortiGate, as long as it is connected to a managed FortiSwitch device.

NEW QUESTION: 10
Which two statements about FortiSwitchmanager are true1? (Choose two)
A. Per-device management is the default management mode on FortiManager
B. FortiManager obtains the FortiSwitch status information by querying the FortiGate REST API every three minutes
C. If the administrator makes any changes on FortiSwitch manager they must also install those changes on FortiGate so that those changes are applied on the managed switches
D. Any switch discovered or authorized on FortiGate must be added manually on FortiSwitch manager
Answer: B,C (LEAVE A REPLY)
Explanation
According to the FortiManager Administration Guide1, "FortiManager obtains the FortiSwitch status information by querying the FortiGate REST API every three minutes." Therefore, option B is true because it describes how FortiManager gets the information about the managed switches. According to the same guide2,
"If you make any changes in this module, you must install them on your managed device so that they are applied on your managed switches." Therefore, option C is true because it describes what the administrator must do after making any changes on FortiSwitch manager. Option A is false because central management is the default management mode on FortiManager, not per-device management. Option D is false because anyswitch discovered or authorized on FortiGate will be automatically added on FortiSwitch manager, not manually.
1: https://docs.fortinet.com/document/fortimanager/7.0.0/administration-guide/734537/fortiswitch-manager 2:
https://docs.fortinet.com/document/fortimanager/7.0.0/administration-guide/734537/fortiswitch-manager#fortisw

NEW QUESTION: 11
An administrator is testing the connectivity for a new VLAN The devices in the VLAN are connected to a FortiSwitch device that is managed by FortiGate Quarantine is disabled on FortiGate While testing the administrator noticed that devices can ping FortiGate and FortiGate can ping the devices The administrator also noticed that inter-VLAN communication works However intra-VLAN communication does not work Which scenario is likely to cause this issue?
A. Access VLAN is enabled on the VLAN
B. The native VLAN configured on the ports is incorrect
C. The FortiSwitch MAC address table is missing entries
D. The FortiGate ARP table is missing entries
Answer: C (LEAVE A REPLY)
Explanation
According to the scenario, the devices in the VLAN are connected to a FortiSwitch device that is managed by FortiGate. Quarantine is disabled on FortiGate, which means that the devices are not blocked by any security policy. The devices can ping FortiGate and FortiGate can ping the devices, which means that the IP connectivity is working. Inter-VLAN communication works, which means that the routing between VLANs is working. However, intra-VLAN communication does not work, which means that the switching within the VLAN is not working. Therefore, option C is true because the FortiSwitch MAC address table is missing entries, which means that the FortiSwitch does not know how to forward frames to the destination MAC addresses within the VLAN. Option A is false because access VLAN is enabled on the VLAN, which means that the VLAN ID is added to the frames on ingress and removed on egress. This does not affect intra-VLAN communication. Option B is false because the native VLAN configured on the ports is incorrect, which means that the frames on the native VLAN are not tagged with a VLAN ID. This does not affect intra-VLAN communication. Option D is false because the FortiGate ARP table is missing entries, which means that FortiGate does not know how to map IP addresses to MAC addresses. This does not affect intra-VLAN communication.

NEW QUESTION: 12
Refer to the exhibit
Examine the sections of the configuration shown in the output
What action will FortiGate take when verifying the student certificate through OCSP?
A. Reject the student certificate if the OCSP server replies that the student certificate status is unknown
B. Not verify the OCSP server certificate
C. Use the OCSP URL included in the student certificate to verify the student certificate
D. Consider the student certificate status as valid if the OCSP server is unreachable
Answer: (SHOW ANSWER)
Explanation
According to the exhibit, the FortiGate configuration has ocsp-status enabled and ocsp-option set to certificate.

This means that FortiGate will use OCSP to verify the revocation status of certificates presented by clients. According to the FortiGate Administration Guide2, "If you select certificate, FortiGate uses an OCSP URL included in a certificate to verify that certificate." Therefore, option C is true because it describes what action FortiGate will take when verifying the student certificate through OCSP. Option A is false because FortiGate will not reject the student certificate if the OCSP server replies that the student certificate status is unknown, but rather accept it as valid. Option B is false because FortiGate will verify the OCSPserver certificate by default, unless strict-ocsp-check is disabled. Option D is false because FortiGate will not consider the student certificate status as valid if the OCSP server is unreachable, but rather reject it as invalid.

NEW QUESTION: 13
Refer to the exhibit
Examine the FortiGate RSSO configuration shown in the exhibit
FortiGate is configured to receive RADIUS accounting messages on port3 to authenticate RSSO users The users are located behind port3 and the internet link is connected to port1 FortiGate is processing incoming RADIUS accounting messages successfully and RSSO users are getting associated with the RSSO Group user group However all the users are able to access the internet, and the administrator wants to restrict internet access to RSSO users only Which configuration change should the administrator make to fix the problem?
A. Enable Security Fabric Connection on port3
B. Create a second firewall policy from port3 lo port1 and select the target destination subnets
C. Add RSSO Group to the firewall policy
D. Change the RADIUS Attribute Value selling to match the name of the RADIUS attribute containing the group membership information of the RSSO users
Answer: C (LEAVE A REPLY)
Explanation
According to the exhibit, the firewall policy from port3 to port1 has no user group specified, which means that it allows all users to access the internet. Therefore, option B is true because adding RSSO Group to the firewall policy will restrict internet access to RSSO users only. Option A is false because changing the RADIUS Attribute Value setting will not affect the firewall policy, but rather the RSSO user group membership. Option C is false because enabling Security Fabric Connection on port3 will not affect the firewall policy, but rather the communication between FortiGate and other Security Fabric devices. Option D is false because creating a second firewall policy from port3 to port1 will not affect the existing firewall policy, but rather create a redundant or conflicting policy.

been corrected get the **newest** Actual4test.com NSE7_LED-7.0 dumps with Test Engine here: https://www.actual4test.com/NSE7_LED-7.0_examcollection.html (**63** Q&As Dumps, **30%OFF Special Discount: Freepdfdumps**)