

Fortinet

Exam Questions NSE7_LED-7.0

Fortinet NSE 7 - LAN Edge 7.0



NEW QUESTION 1

Which FortiSwitch VLANs are automatically created on FortGate when the first FortiSwitch device is discovered1?

- A. default quarantine, rspan voice video onboarding and nac_segment
- B. access, quarantine, rspa
- C. voice, video, and onboarding
- D. default quarantine rspan voice video and nac_segment
- E. fortilin
- F. quarantine erspan voice video and onboarding

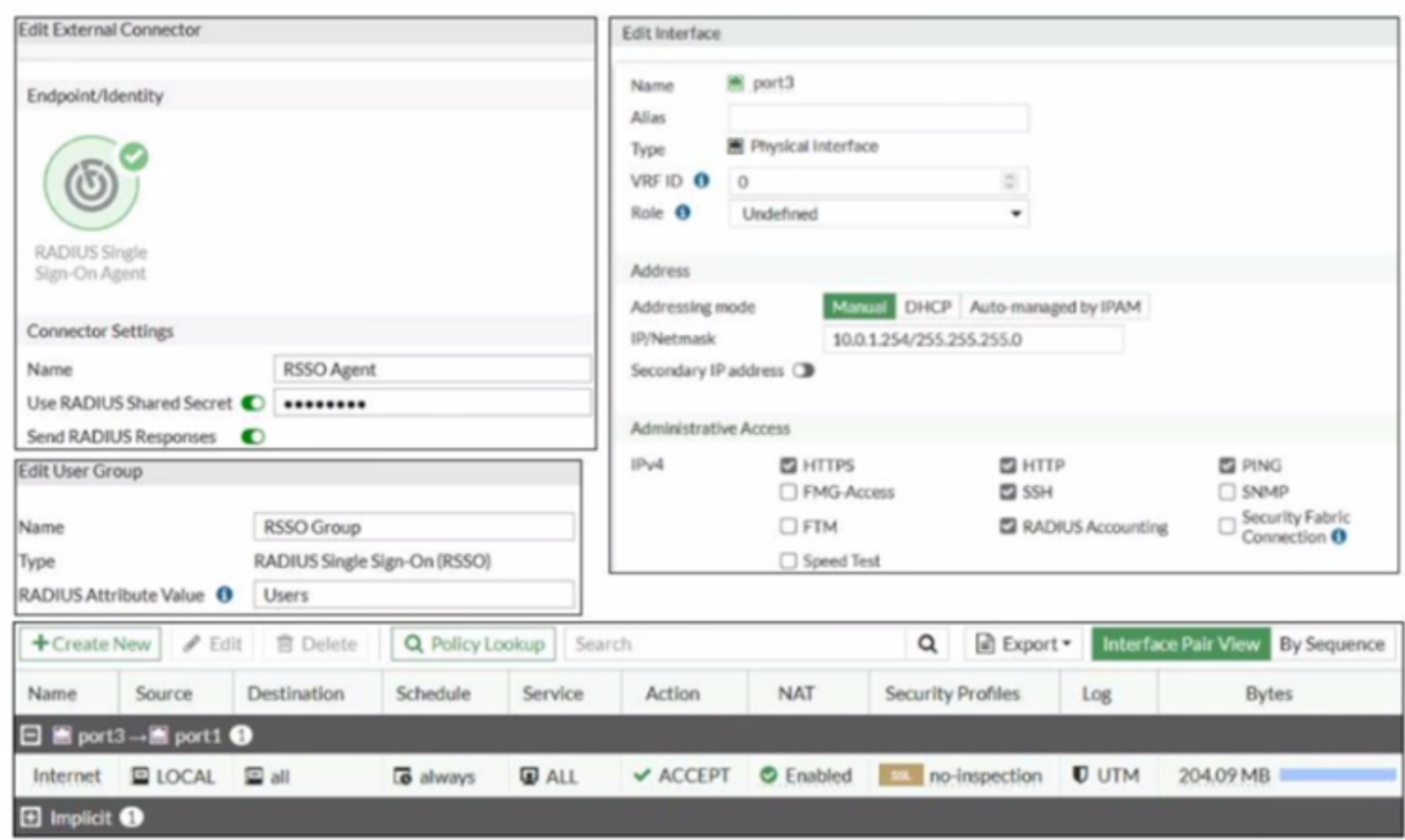
Answer: D

Explanation:

According to the FortiGate Administration Guide, “When you add a FortiSwitch device to the Security Fabric, FortiGate automatically creates the following VLANs on theFortiSwitch device: fortilink, quarantine, erspan, voice, video, and onboarding.” Therefore, option D is true because it lists the FortiSwitch VLANs that are automatically created on FortiGate when the first FortiSwitch device is discovered. Option A is false because default and nac_segment are not among the automatically created VLANs. Option B is false because access and rspan are not among the automatically created VLANs. Option C is false because default and nac_segment are not among the automatically created VLANs.

NEW QUESTION 2

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. Change the RADIUS Attribute Value selling to match the name of the RADIUS attribute containing the group membership information of the RSSO users
- B. Add RSSO Group to the firewall policy
- C. Enable Security Fabric Connection on port3
- D. Create a second firewall policy from port3 lo port1 and select the target destination subnets

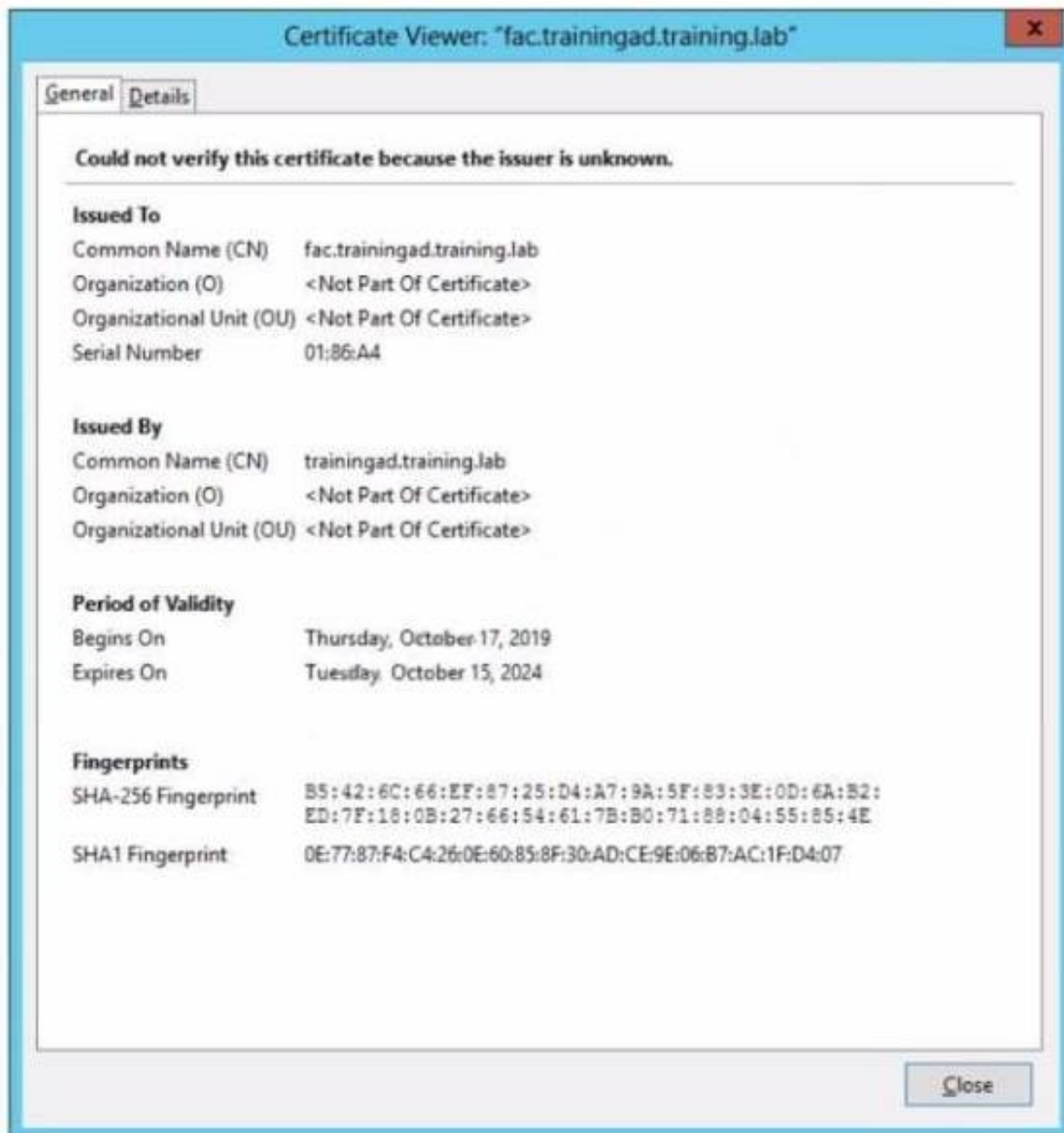
Answer: B

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.

NEW QUESTION 3

Refer to the exhibit



Wireless guest users are unable to authenticate because they are getting a certificate error while loading the captive portal login page. This URL string is the HTTPS POST URL guest wireless users see when attempting to access the network using the web browser

```
https://fac.trainingad.training.com/guest/login/?
loginpost=https://auth.trainingad.training.lab/1003/fqauthmagic=00a030293d1f411ausermac=b8:27:eb:d8:50:72&ipmac=70:4c:a5:f5:0d:28&ip=10.10.100.2&userip=10.0.3.1&ssid=Guest03&apname=0822127718000148&ssid=70:4c:a5:9d:0d:30
```

Which two settings are the likely causes of the issue? (Choose two.)

- A. The external server FQDN is incorrect
- B. The wireless user's browser is missing a CA certificate
- C. The FortiGate authentication interface address is using HTTPS
- D. The user address is not in DDNS form

Answer: AB

Explanation:

According to the exhibit, the wireless guest users are getting a certificate error while loading the captive portal login page. This means that the browser cannot verify the identity of the server that is hosting the login page. Therefore, option A is true because the external server FQDN is incorrect, which means that it does not match the common name or subject alternative name of the server certificate. Option B is also true because the wireless user's browser is missing a CA certificate, which means that it does not have the root or intermediate certificate that issued the server certificate. Option C is false because the FortiGate authentication interface address is using HTTPS, which is a secure protocol that encrypts the communication between the browser and the server. Option D is false because the user address is not in DDNS form, which is not related to the certificate error.

NEW QUESTION 4

Which two statements about MAC address quarantine by redirect mode are true? (Choose two)

- A. The quarantined device is moved to the quarantine VLAN
- B. The device MAC address is added to the Quarantined Devices firewall address group
- C. It is the default mode for MAC address quarantine
- D. The quarantined device is kept in the current VLAN

Answer: BD

Explanation:

According to the FortiGate Administration Guide, "MAC address quarantine by redirect mode allows you to quarantine devices by adding their MAC addresses to a firewall address group called Quarantined Devices. The quarantined devices are kept in their current VLANs, but their traffic is redirected to a quarantine portal." Therefore, options B and D are true because they describe the statements about MAC address quarantine by redirect mode. Option A is false because the quarantined device is not moved to the quarantine VLAN, but rather kept in the current VLAN. Option C is false because redirect mode is not the default mode for MAC address quarantine, but rather an alternative mode that can be enabled by setting mac-quarantine-mode to redirect.

<https://docs.fortinet.com/document/fortiap/7.0.0/configuration-guide/734537/radius-authenticated-dynamic-vlan>

: <https://docs.fortinet.com/document/fortigate/7.0.0/administration-guide/734537/mac-address-quarantine>

NEW QUESTION 5

Refer to the exhibit.

Examine the FortiSwitch security policy shown in the exhibit

If the security profile shown in the exhibit is assigned to all ports on a FortiSwitch device for 802.1X authentication which statement about the switch is correct?

- A. FortiSwitch cannot authenticate multiple devices connected to the same port
- B. FortiSwitch will try to authenticate non-802.1X devices using the device MAC address as the username and password
- C. FortiSwitch will assign non-802.1X devices to the onboarding VLAN
- D. All EAP messages will be terminated on FortiSwitch

Answer: C

Explanation:

According to the FortiSwitch Administration Guide, "If a device does not support 802.1X authentication, you can configure the switch to assign the device to an onboarding VLAN. The onboarding VLAN is a separate VLAN that you can use to provide limited network access to non-802.1X devices." Therefore, option C is true because it describes the behavior of FortiSwitch when the security profile shown in the exhibit is assigned to all ports. Option A is false because FortiSwitch can authenticate multiple devices connected to the same port using MAC-based or MAB-EAP modes. Option B is false because FortiSwitch will not try to authenticate non-802.1X devices using the device MAC address as the username and password, but rather use MAC authentication bypass (MAB) or EAP pass-through modes. Option D is false because all EAP messages will be terminated on FortiGate, not FortiSwitch, when using 802.1X authentication.

NEW QUESTION 6

Which two statements about FortiSwitchmanager are true? (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: BC

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 any switch 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 7

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

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 8

Refer to the exhibit

```
FortiGate # diagnose switch-controller switch-info 802.1X
Managed Switch : S224EPTF19006016

port2 : Mode: port-based (mac-by-pass disable)
Link: Link up
Port State: unauthorized: ( )
Dynamic Authorized Vlan : 0
Dynamic Allowed Vlan list:
Dynamic Untagged Vlan list:
EAP pass-through : Enable
EAP egress-frame-tagged : Enable
EAP auto-untagged-vlans : Enable
Allow MAC Move : Disable
Dynamic Access Control List : Disable
Quarantine VLAN (4093) detection : Enable
Native Vlan : 10
Allowed Vlan list: 10,4093
Untagged Vlan list: 4093
Guest VLAN :
Auth-Fail Vlan :
AuthServer-Timeout Vlan :

Sessions info:
00:09:0f:02:02:02      Type=802.1x,,state=AUTHENTICATING,etime=0,eap_cnt=0 params:reAuth=3600
```

A device connected to port2 on FortiSwitch cannot access the network. The port is assigned a security policy to enforce 802.1X authentication. While troubleshooting the issue, the administrator obtains the debug output shown in the exhibit. Which two scenarios are likely to cause this issue? (Choose two.)

- A. The device is not configured for 802.1X authentication.
- B. The device has been quarantined for 3600 seconds.
- C. The device has been assigned the guest VLAN.
- D. The device does not support 802.1X authentication.

Answer: AD**Explanation:**

According to the exhibit, the debug output shows that the device connected to port2 on FortiSwitch is sending an EAPOL-Start message, which is the first step of the 802.1X authentication process. However, the output also shows that the device is not sending any EAP-Response messages, which are required to complete the authentication process. Therefore, option A is true because the device is not configured for 802.1X authentication, which means that it does not have the correct credentials or settings to authenticate with the RADIUS server. Option D is also true because the device does not support 802.1X authentication, which means that it does not have the capability or software to perform 802.1X authentication. Option B is false because the device has not been quarantined for 3600 seconds, but rather has a session timeout of 3600 seconds, which is the default value for 802.1X sessions. Option C is false because the device has not been assigned the guest VLAN, but rather has been assigned the default VLAN, which is VLAN 1.

NEW QUESTION 9

You are setting up an SSID (VAP) to perform RADIUS-authenticated dynamic VLAN allocation. Which three RADIUS attributes must be supplied by the RADIUS server to enable successful VLAN allocation? (Choose three.)

- A. Tunnel-Private-Group-ID
- B. Tunnel-Pvt-Group-ID
- C. Tunnel-Preference
- D. Tunnel-Type
- E. Tunnel-Medium-Type

Answer: ADE**Explanation:**

According to the FortiAP Configuration Guide, "To perform RADIUS-authenticated dynamic VLAN allocation, the RADIUS server must supply the following RADIUS attributes: Tunnel-Private-Group-ID, which specifies the VLAN ID to assign to the user. Tunnel-Type, which specifies the tunneling protocol used for the VLAN. The value must be 13 (VLAN). Tunnel-Medium-Type, which specifies the transport medium used for the VLAN. The value must be 6 (802). Therefore, options A, D, and E are true because they describe the RADIUS attributes that must be supplied by the RADIUS server to enable successful VLAN allocation. Option B is false because Tunnel-Pvt-Group-ID is not a valid RADIUS attribute name, but rather a typo for Tunnel-Private-Group-ID. Option C is false because Tunnel-Preference is not a required RADIUS attribute for dynamic VLAN allocation, but rather an optional attribute that specifies the priority of the VLAN.

NEW QUESTION 10

Refer to the exhibit

```
config vpn certificate ocsf-server
  edit "FAC"
    set url "http://10.0.1.150:2560"
    set cert "CA_Cert_1"
    set unavail-action revoke
  next
end
config vpn certificate setting
  set ocsf-status enable
  set ocsf-option server
  set ocsf-default-server "FAC"
  set strict-ocsf-check enable
end
config user peer
  edit "student"
    set ca "CA_Cert_1"
  next
end
```

Examine the sections of the configuration shown in the output

What action will FortiGate take when verifying the student certificate through OCSF?

- A. Reject the student certificate if the OCSF server replies that the student certificate status is unknown
- B. Not verify the OCSF server certificate
- C. Use the OCSF URL included in the student certificate to verify the student certificate
- D. Consider the student certificate status as valid if the OCSF server is unreachable

Answer: C

Explanation:

According to the exhibit, the FortiGate configuration has ocsf-status enabled and ocsf-option set to certificate.

This means that FortiGate will use OCSF to verify the revocation status of certificates presented by clients. According to the FortiGate Administration Guide2, "If you select certificate, FortiGate uses an OCSF 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 OCSF. Option A is false because FortiGate will not reject the student certificate if the OCSF server replies that the student certificate status is unknown, but rather accept it as valid. Option B is false because FortiGate will verify the OCSFserver certificate by default, unless strict-ocsf-check is disabled. Option D is false because FortiGate will not consider the student certificate status as valid if the OCSF server is unreachable, but rather reject it as invalid.

NEW QUESTION 10

Refer to the exhibit.

```
config system dhcp server
  edit 1
    set ntp-service local
    set default-gateway 169.254.1.1
    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
```

By default FortiOS creates the following DHCP server scope for the FortiLink interface as shown in the exhibit

What is the objective of the vci-string setting?

- A. To ignore DHCP requests coming from FortiSwitch and FortiExtender devices
- B. To reserve IP addresses for FortiSwitch and FortiExtender devices
- C. To restrict the IP address assignment to FortiSwitch and FortiExtender devices
- D. To restrict the IP address assignment to devices that have FortiSwitch or FortiExtender as their hostname

Answer: C

Explanation:

According to the exhibit, the DHCP server scope for the FortiLink interface has a vci-string setting with the value "Cisco AP c2700". This setting is used to match the vendor class identifier (VCI) of the DHCP clients that request an IP address from the DHCP server. The VCI is a text string that uniquely identifies a type of vendor device. Therefore, option C is true because the vci-string setting restricts the IP address assignment to FortiSwitch and FortiExtender devices, which use the VCI "Cisco AP c2700". Option A is false because the vci-string setting does not ignore DHCP requests coming from FortiSwitch and FortiExtender devices, but rather accepts them. Option B is false because the vci-string setting does not reserve IP addresses for FortiSwitch and FortiExtender devices, but rather assigns them dynamically. Option D is false because the vci-string setting does not restrict the IP address assignment to devices that have FortiSwitch or FortiExtender as their hostname, but rather to devices that have "Cisco AP c2700" as their VCI.

NEW QUESTION 15

Refer to the exhibits.

Firewall Policy

```
config firewall policy
  edit 11
    set name "Guest to Internal"
    set uuid c5e45130-aada-51e8-ee0c-bc1204f9f163
    set srcintf "guest"
    set dstintf "port3"
    set srcaddr "all"
    set dstaddr "FortiAuthenticator" "WindowsAD"
    set action accept
    set schedule "always"
    set service "ALL"
  next
end
```

Examine the firewall policy configuration and SSID settings

An administrator has configured a guest wireless network on FortiGate using the external captive portal. The administrator has verified that the external captive portal URL is correct. However, wireless users are not able to see the captive portal login page. Given the configuration shown in the exhibit and the SSID settings, which configuration change should the administrator make to fix the problem?

- A. Disable the user group from the SSID configuration
- B. Enable the captive-portal-exempt option in the firewall policy with the ID 11.
- C. Apply a guest.portal user group in the firewall policy with the ID 11.
- D. Include the wireless client subnet range in the Exempt Source section

Answer: C

Explanation:

According to the FortiGate Administration Guide, "To use an external captive portal, you must configure a user group that uses the external captive portal as the authentication method and apply it to a firewall policy." Therefore, option C is true because it will allow the wireless users to be redirected to the external captive portal URL when they try to access the Internet. Option A is false because disabling the user group from the SSID configuration will prevent the wireless users from being authenticated by the FortiGate device. Option B is false because enabling the captive-portal-exempt option in the firewall policy will bypass the captive portal authentication for the wireless users, which is not the desired outcome. Option D is false because including the wireless client subnet range in the Exempt Source section will also bypass the captive portal authentication for the wireless users, which is not the desired outcome.

NEW QUESTION 20

When you configure a FortiAP wireless interface for auto TX power control, which statement describes how it configures its transmission power?"

- A. Every 30 seconds the AP will measure the signal strength of the AP using the client. The AP will adjust its signal strength up or down until the AP signal is detected at -70 dBm.
- B. Every 30 seconds FortiGate measures the signal strength of adjacent AP interfaces. It will adjust its own AP power to match the adjacent AP signal strength.
- C. Every 30 seconds FortiGate measures the signal strength of adjacent FortiAP interfaces. It will adjust the adjacent AP power to be detectable at -70 dBm.
- D. Every 30 seconds FortiGate measures the signal strength of the weakest associated client. The AP will then configure its radio power to match the detected signal strength of the client.

Answer: A

Explanation:

According to the FortiAP Configuration Guide, "Auto TX power control allows the AP to adjust its transmit power based on the signal strength of the client. The AP will measure the signal strength of the client every 30 seconds and adjust its transmit power up or down until the client signal is detected at -70 dBm." Therefore, option A is true because it describes how the FortiAP wireless interface configures its transmission power when auto TX power control is enabled. Option B is false because FortiGate does not measure the signal strength of adjacent AP interfaces, but rather the FortiAP does. Option C is false because FortiGate does not adjust the adjacent AP power, but rather the FortiAP adjusts its own power. Option D is false because FortiGate does not measure the signal strength of the weakest associated client, but rather the FortiAP does.

NEW QUESTION 23

Which two statements about the guest portal on FortiAuthenticator are true? (Choose two.)

- A. Each remote user on FortiAuthenticator can sponsor up to 10 guest accounts
- B. Administrators must approve all guest accounts before they can be used
- C. The guest portal provides pre and post-log in services
- D. Administrators can use one or more incoming parameters to configure a mapping rule for the guest portal

Answer: CD

Explanation:

According to the FortiAuthenticator Administration Guide2, "The guest portal provides pre and post-log in services for users (such as password reset and token registration abilities), and rules and replacement messages can be configured." Therefore, option C is true. The same guide also states that "Administrators can use one or more incoming parameters to configure a mapping rule for the guest portal." Therefore, option D is true. Option A is false because remote users can sponsor any number of guest accounts, as long as they do not exceed the maximum number of guest accounts allowed by the license. Option B is false because administrators can choose to approve or reject guest accounts, or enable auto-approval.

NEW QUESTION 27

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: AB

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 apply security 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 28

Refer to the exhibit.

```
FortiGate # diagnose test authserver radius FAC-Lab mschap2 student password
[1909] handle_req-Rcvd auth req 1288058912 for student in FAC-Lab opt=0000001d prot=4
[466] __compose_group_list_from_req-Group 'FAC-Lab', type 1
[617] fnband_pop3_start-student
[505] __fnband_cfg_get_radius_list_by_server-Loading RADIUS server 'FAC-Lab'
[342] fnband_create_radius_socket-Opened radius socket 13
[342] fnband_create_radius_socket-Opened radius socket 14
[1392] fnband_radius_auth_send-Compose RADIUS request
[1352] fnband_rad_dns_cb-10.0.1.150->10.0.1.150
[1330] __fnband_rad_send-Sent radius req to server 'FAC-Lab': fd=13, IP=10.0.1.150(10.0.1.150:1812) code=1 id=2 len=180 us
er="student" using MS-CHAPv2
[320] radius_server_auth-Timer of rad 'FAC-Lab' is added
  33] create_auth_session-Total 1 server(s) to try
  359] fnband_auth_handle_radius_result-Timer of rad 'FAC-Lab' is deleted
  800] fnband_radius_auth_validate_pkt-RADIUS resp code 2
[320] extract_success_vsas-FORTINET attr, type 1, val SSLVPN
[1661] __radius_decode_mppe_key-Key len after decode 16
[1661] __radius_decode_mppe_key-Key len after decode 16

[1385] fnband_auth_handle_radius_result-->Result for radius svr 'FAC-Lab' 10.0.1.150(1) is 0
[266] find_matched_usr_grps-Skipped group matching
[217] fnband_comm_send_result-Sending result 0 (nid 0) for req 1288058912, len=2156
authenticate 'student' against 'mschap2' succeeded, server=primary assigned_rad_session_id=1288058912 session_timeout=0 se
cs idle_timeout=0 secs!
Group membership(s) - SSLVPN
```

Examine the debug output shown in the exhibit

Which two statements about the RADIUS debug output are true" (Choose two)

- A. The user student belongs to the SSLVPN group
- B. User authentication failed
- C. The RADIUS server sent a vendor-specific attribute in the RADIUS response
- D. User authentication succeeded using MSCHAP

Answer: AD

Explanation:

According to the exhibit, the debug output shows a RADIUS debug output from FortiGate. The output shows that FortiGate sent a RADIUS Access-Request packet to FortiAuthenticator with the username student and received a RADIUS Access-Accept packet from FortiAuthenticator with a Class attribute containing SSLVPN. Therefore, option A is true because it indicates that the user student belongs to the SSLVPN group on FortiAuthenticator. The output also shows that FortiGate used MSCHAP as the authentication method and received a MS-MPPE-Send-Key and a MS-MPPE-Recv-Key from FortiAuthenticator. Therefore, option D is true because it indicates that user authentication succeeded using MSCHAP. Option B is false because user authentication did not fail, but rather succeeded. Option C is false because FortiAuthenticator did not send a vendor-specific attribute in the RADIUS response, but rather standard attributes defined by RFCs.

NEW QUESTION 32
.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions and Answers in PDF Format

NSE7_LED-7.0 Practice Exam Features:

- * NSE7_LED-7.0 Questions and Answers Updated Frequently
- * NSE7_LED-7.0 Practice Questions Verified by Expert Senior Certified Staff
- * NSE7_LED-7.0 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * NSE7_LED-7.0 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The NSE7_LED-7.0 Practice Test Here](#)