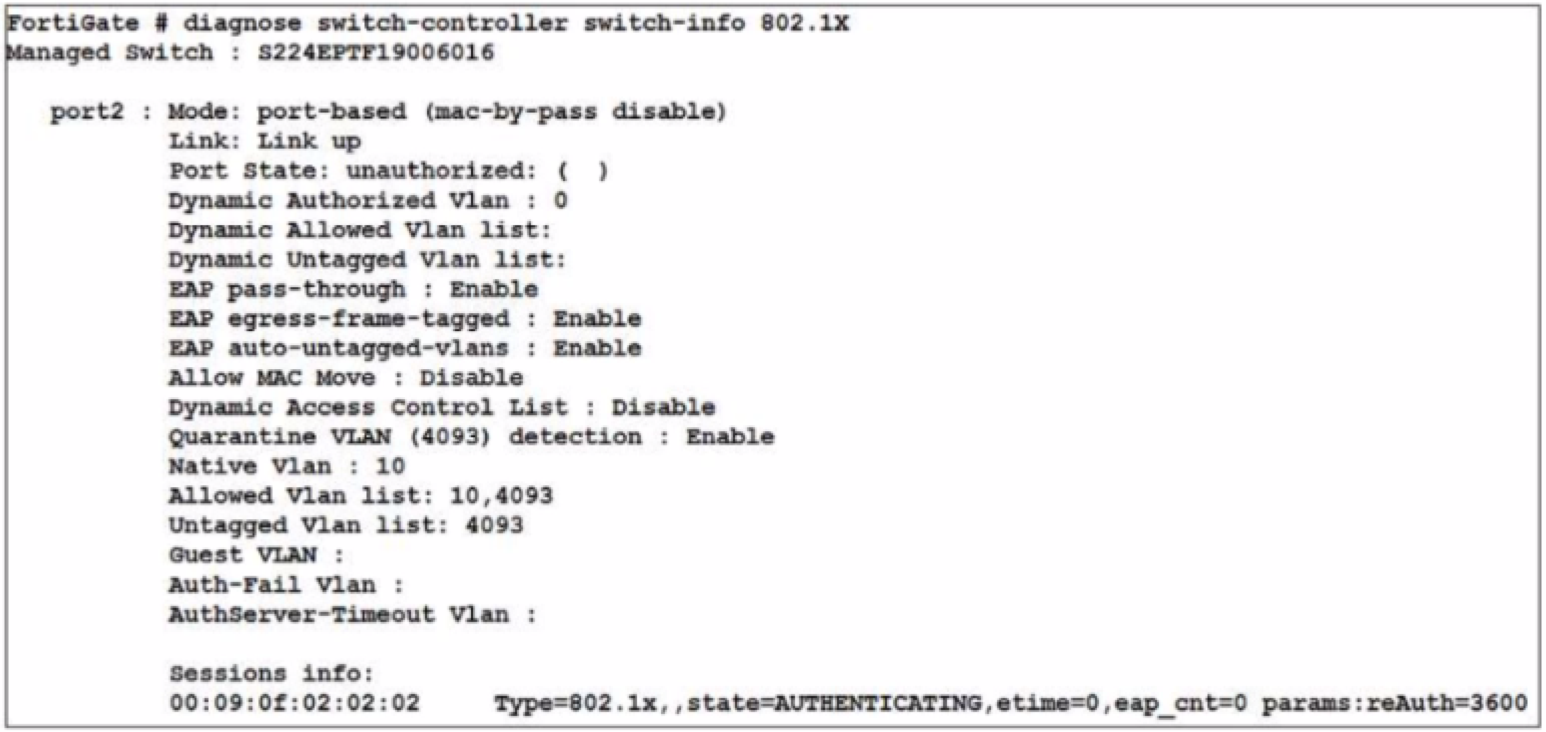
Free Questions for NSE7_LED-7.0 by go4braindumps

Shared by Mcclure on 22-07-2024

Question 1

Question Type: MultipleChoice

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.)

Options:

A- The device is not configured for 802 IX 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:

A, D

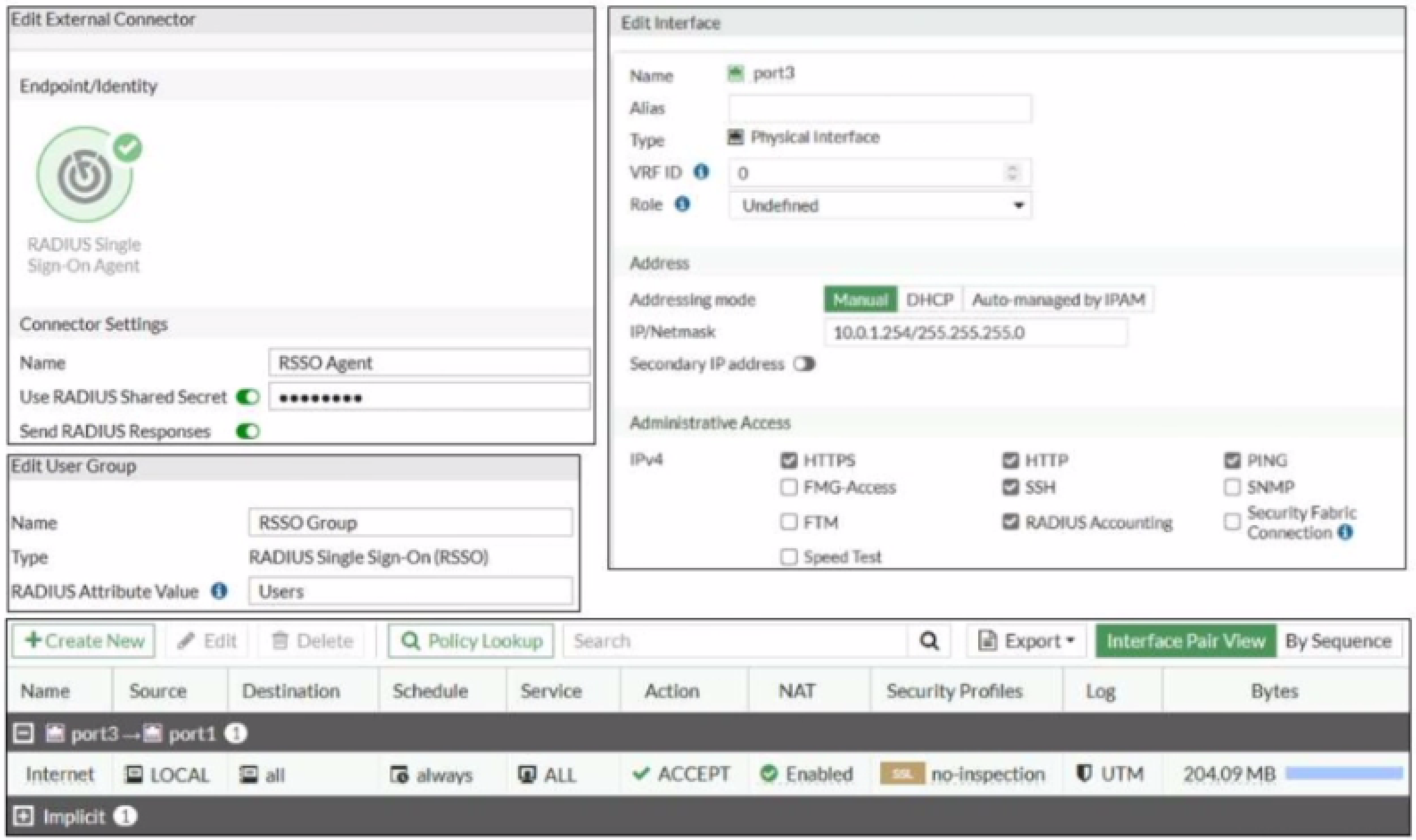
Explanation:

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.

Question 2

Question Type: MultipleChoice

Refer to the exhibit



Edit External Connector

Endpoint/Identity

RADIUS Single Sign-On Agent

Connector Settings

Name	RSSO Agent
Use RADIUS Shared Secret ●	•••••••••
Send RADIUS Responses ●	

Edit User Group

Name	RSSO Group
Type	RADIUS Single Sign-On (RSSO)
RADIUS Attribute Value	Users

Edit Interface

Name	port3
Alias	
Type	Physical Interface
VRF ID	0
Role	Undefined

Address

Addressing mode	[✓ Manual] DHCP Auto-managed by IPAM
IP/Netmask	10.0.1.254/255.255.255.0
Secondary IP address ○	

Administrative Access

IPv4	☑ HTTPS	☑ HTTP	☑ PING
	☐ FMG-Access	☑ SSH	☐ SNMP
	☐ FTM	☑ RADIUS Accounting	☐ Security Fabric Connection
	☐ Speed Test		

Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
⊟ port3 → port1 1									
Internet	LOCAL	all	always	ALL	✓ ACCEPT	Enabled	SSL no-inspection	UTM	204.09 MB
⊞ Implicit 1									

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?

Options:

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

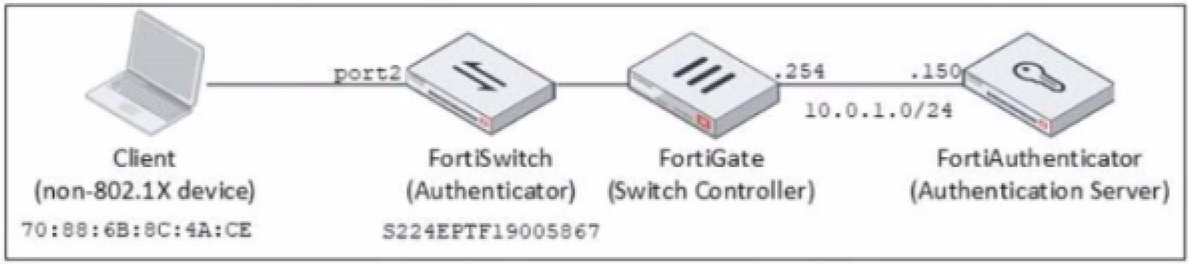
Explanation:

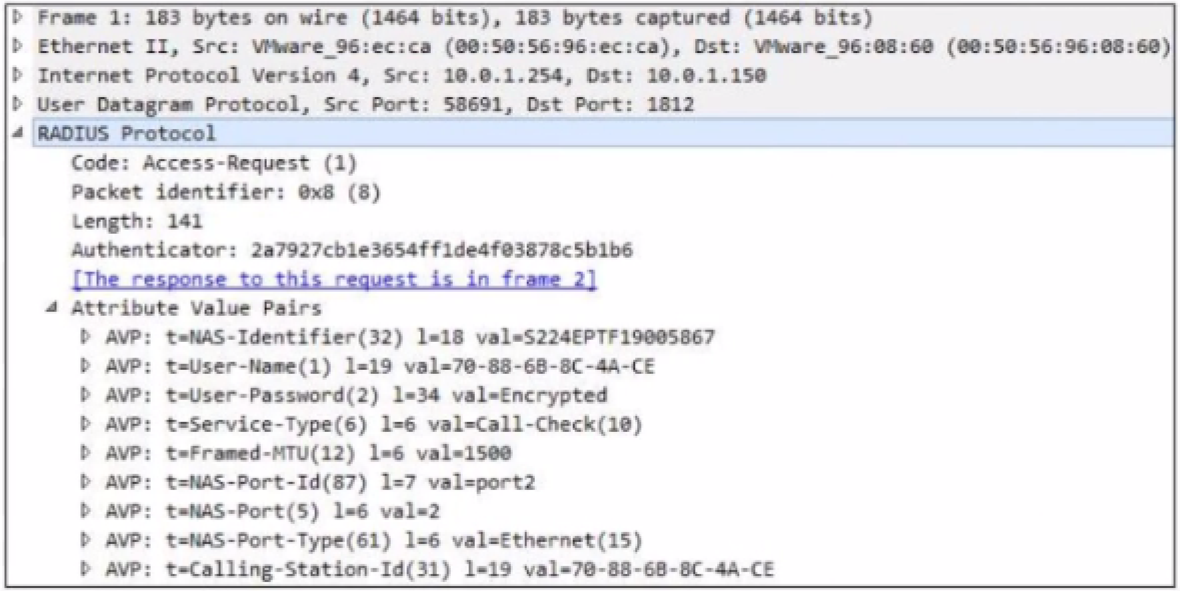
According to the exhibit, the firewall policy from port3 to port1 has no user group specified, which means that it allows all users to access the internet. Therefore, option B is true because adding RSSO Group to the firewall policy will restrict internet access to RSSO users only. Option A is false 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.

Question 3

Question Type: MultipleChoice

Refer to the exhibit.





```
▷ Frame 1: 183 bytes on wire (1464 bits), 183 bytes captured (1464 bits)
▷ Ethernet II, Src: VMware_96:ec:ca (00:50:56:96:ec:ca), Dst: VMware_96:08:60 (00:50:56:96:08:60)
▷ Internet Protocol Version 4, Src: 10.0.1.254, Dst: 10.0.1.150
▷ User Datagram Protocol, Src Port: 58691, Dst Port: 1812
◢ RADIUS Protocol
    Code: Access-Request (1)
    Packet identifier: 0x8 (8)
    Length: 141
    Authenticator: 2a7927cb1e3654ff1de4f03878c5b1b6
    [The response to this request is in frame 2]
  ◢ Attribute Value Pairs
    ▷ AVP: t=NAS-Identifier(32) l=18 val=S224EPTF19005867
    ▷ AVP: t=User-Name(1) l=19 val=70-88-6B-8C-4A-CE
    ▷ AVP: t=User-Password(2) l=34 val=Encrypted
    ▷ AVP: t=Service-Type(6) l=6 val=Call-Check(10)
    ▷ AVP: t=Framed-MTU(12) l=6 val=1500
    ▷ AVP: t=NAS-Port-Id(87) l=7 val=port2
    ▷ AVP: t=NAS-Port(5) l=6 val=2
    ▷ AVP: t=NAS-Port-Type(61) l=6 val=Ethernet(15)
    ▷ AVP: t=Calling-Station-Id(31) l=19 val=70-88-6B-8C-4A-CE
```

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?

Options:

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

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.

Question 4

Question Type: MultipleChoice

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

Options:

A- default quarantine, rspan voice video onboarding and nac_segment

B- access, quarantine, rspan. voice, video, and onboarding

C- default quarantine rspan voice video and nac_segment

D- fortilink. quarantine erspan voice video and onboarding

Answer:

D

Explanation:

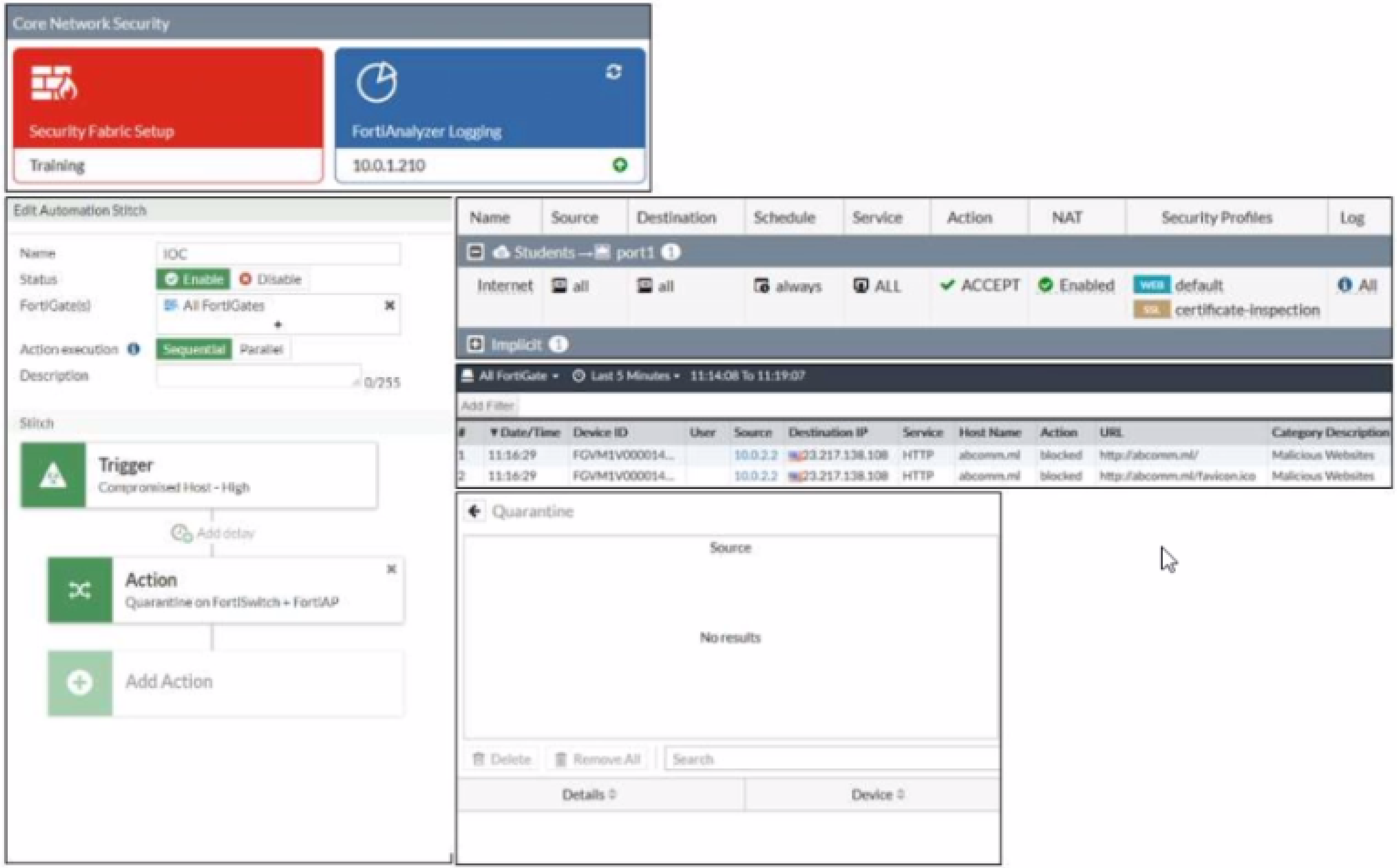
According to the FortiGate Administration Guide, ''When you add a FortiSwitch device to the Security Fabric, FortiGate automatically creates the following VLANs on the FortiSwitch device: fortilink, quarantine, erspan, voice, video, and onboarding.'' Therefore, option D is true because it lists the FortiSwitch 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.

Question 5

Question Type: MultipleChoice

Refer to the exhibit.



Core Network Security

Security Fabric Setup

Training

FortiAnalyzer Logging

10.0.1.210

Edit Automation Stitch

Name	IOC
Status	Enable Disable
FortiGate(s)	All FortiGates
Action execution	Sequential Parallel
Description	0/255

Stitch

Trigger
Compromised Host - High

Add delay

Action
Quarantine on FortiSwitch + FortiAP

Add Action

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

All FortiGate ▾ Last 5 Minutes ▾ 11:14:08 To 11:19:07

Add Filter

#	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.ml	blocked	http://abcomm.ml/	Malicious Websites
2	11:16:29	FGVM1V000014...		10.0.2.2	23.217.138.108	HTTP	abcomm.ml	blocked	http://abcomm.ml/favicon.ico	Malicious Websites

Quarantine

Source

No results

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)

Options:

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:

B, D

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.

Question 6

Question Type: MultipleChoice

Which EAP method requires the use of a digital certificate on both the server end and the client end?

Options:

A- EAP-TTLS

B- PEAP

C- EAP-GTC

D- EAP-TLS

Answer:

D

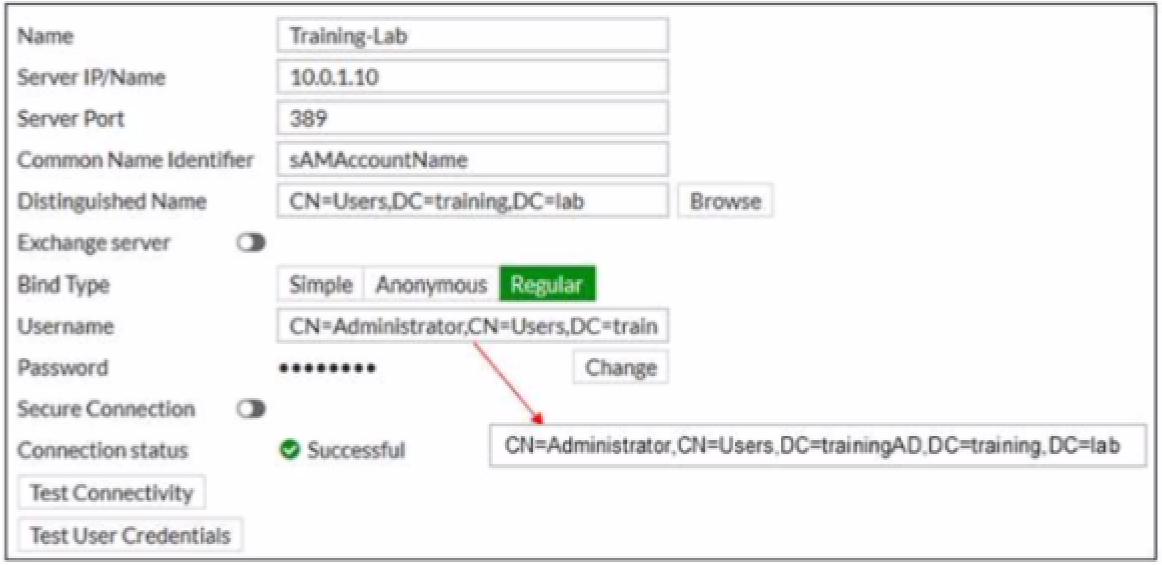
Explanation:

According to the FortiGate Administration Guide, "EAP-TLS is the most secure EAP method. It requires a digital certificate on both the server end and the client end. The server and client authenticate each other using their certificates." Therefore, option D is true because it describes the EAP method that requires the use of a digital certificate on both the server end and the client end. Option A is false because EAP-TTLS only requires a digital certificate on the server end, not the client end. Option B is false because PEAP also only requires a digital certificate on the server end, not the client end. Option C is false because EAP-GTC does not require a digital certificate on either the server end or the client end.

Question 7

Question Type: **MultipleChoice**

Refer to the exhibit.



Name: Training-Lab

Server IP/Name: 10.0.1.10

Server Port: 389

Common Name Identifier: sAMAccountName

Distinguished Name: CN=Users,DC=training,DC=lab

Exchange server: ○

Bind Type: Simple | Anonymous | **Regular**

Username: CN=Administrator,CN=Users,DC=train

Password: •••••••••

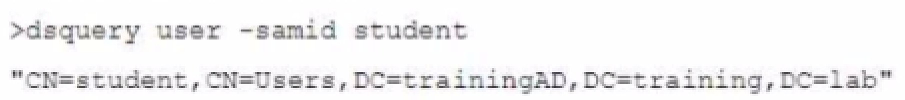
Secure Connection: ○

Connection status: ✓ Successful

CN=Administrator,CN=Users,DC=trainingAD,DC=training,DC=lab

Examine the LDAP server configuration shown in the exhibit Note that the Username setting has been expanded to display Its full content

On the Windows AD server 10.0.1.10, the administrator used dsquery. which returned the following output:



```
>dsquery user -samid student

"CN=student,CN=Users,DC=trainingAD,DC=training,DC=lab"
```

According to the output which FortiGate LDAP setting is configured incorrectly"

Options:

A- Common Name Identifier

B- Bind Type

C- Distinguished Name

D- Username

Answer:

C

Explanation:

According to the exhibits, the LDAP server configuration on FortiGate has the Distinguished Name set to "dc=training,dc=lab". However, according to the output of the dsquery command on the Windows AD server, the Distinguished Name of the domain should be "dc=trainingAD,dc=training,dc=lab". Therefore, option C is true because the Distinguished Name on FortiGate is configured incorrectly and does not match the actual Distinguished Name of the domain. Option A is false because the Common Name Identifier on FortiGate is configured correctly as "cn". Option B is false because the Bind Type on FortiGate is configured correctly as "Regular". Option D is false because the Username on FortiGate is configured correctly as "cn=admin,cn=users,dc=trainingAD,dc=training,dc=lab".

Question 8

Question Type: **MultipleChoice**

Where can FortiGate learn the FortiManager IP address or FQDN for zero-touch provisioning'?

Options:

A- From an LDAP server using a simple bind operation

B- From a TFTP server

C- From a DHCP server using options 240 and 241

D- From a DNS server using A or AAAA records

Answer:

D

Explanation:

According to the FortiGate Administration Guide, "FortiGate can learn the FortiManager IP address or FQDN for zero-touch provisioning from a DNS server using A or AAAA records. The DNS server must be configured to resolve the hostname fortimanager.fortinet.com to the IP address or FQDN of the FortiManager device." Therefore, option D is true because it describes the method for FortiGate to learn the FortiManager IP address or FQDN for zero-touch provisioning. Option A is false because LDAP is not used for zero-touch provisioning. Option B is false because TFTP is not used for zero-touch provisioning. Option C is false because DHCP options 240 and 241 are not used for zero-touch provisioning.

Question 9

Question Type: MultipleChoice

Which two statements about the MAC-based 802 1X security mode available on FortiSwitch are true? (Choose two.)

Options:

A- FortiSwitch authenticates a single device and opens the port to other devices connected to the port

B- FortiSwitch authenticates each device connected to the port

C- It cannot be used in conjunction with MAC authentication bypass

D- FortiSwitch can grant different access levels to each device connected to the port

Answer:

B, D

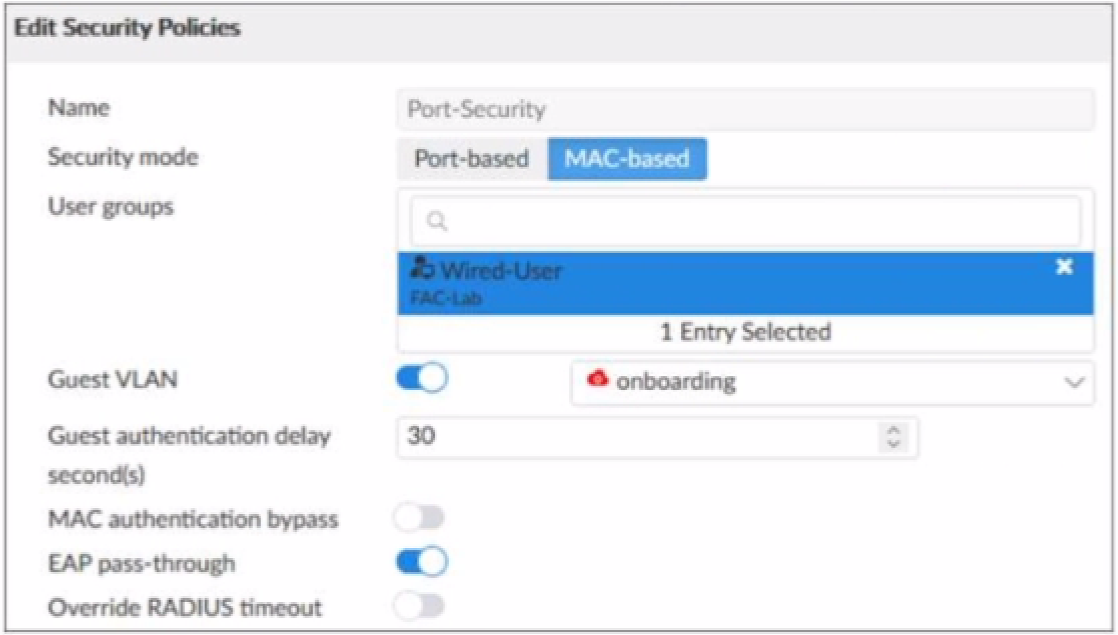
Explanation:

According to the FortiSwitch Administration Guide, ''MAC-based 802.1X security mode allows you to authenticate each device connected to a port using its MAC address as the username and password.'' Therefore, option B is true because it describes the MAC-based 802.1X security mode available on FortiSwitch. Option D is also true because FortiSwitch can grant different access levels to each device connected to the port based on the user group and security policy assigned to them. Option A is false because FortiSwitch does not authenticate a single device and open the port to other devices connected to the port, but rather authenticates each device individually. Option C is false because MAC-based 802.1X security mode can be used in conjunction with MAC authentication bypass (MAB) or EAP pass-through modes, which are fallback options for non-802.1X devices.

Question 10

Question Type: MultipleChoice

Refer to the exhibit.



Edit Security Policies

Name: Port-Security

Security mode: Port-based | MAC-based (selected)

User groups: Wired-User (FAC-Lab)

1 Entry Selected

Guest VLAN: enabled, onboarding

Guest authentication delay second(s): 30

MAC authentication bypass: disabled

EAP pass-through: enabled

Override RADIUS timeout: disabled

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?

Options:

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

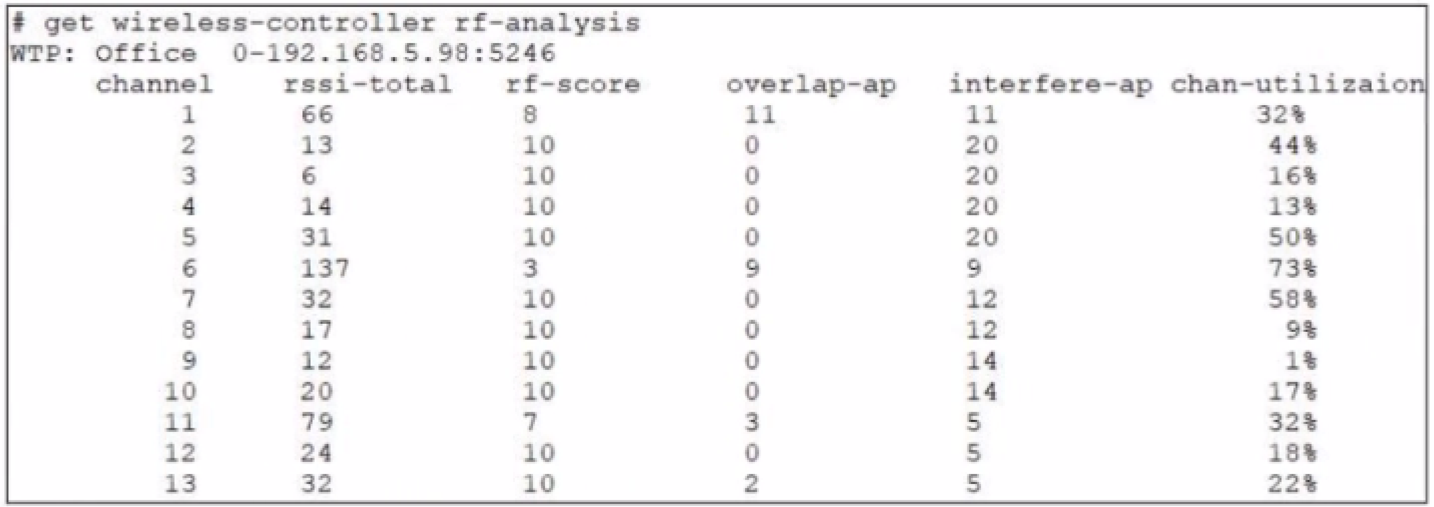
Explanation:

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.

Question 11

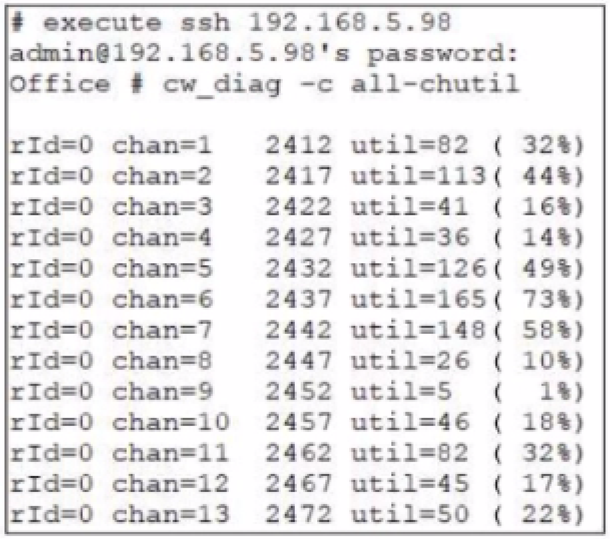
Question Type: MultipleChoice

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.



```
# execute ssh 192.168.5.98
admin@192.168.5.98's password:
Office # cw_diag -c all-chutil

rId=0 chan=1   2412 util=82 ( 32%)
rId=0 chan=2   2417 util=113( 44%)
rId=0 chan=3   2422 util=41 ( 16%)
rId=0 chan=4   2427 util=36 ( 14%)
rId=0 chan=5   2432 util=126( 49%)
rId=0 chan=6   2437 util=165( 73%)
rId=0 chan=7   2442 util=148( 58%)
rId=0 chan=8   2447 util=26 ( 10%)
rId=0 chan=9   2452 util=5  (  1%)
rId=0 chan=10  2457 util=46 ( 18%)
rId=0 chan=11  2462 util=82 ( 32%)
rId=0 chan=12  2467 util=45 ( 17%)
rId=0 chan=13  2472 util=50 ( 22%)
```

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?

Options:

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

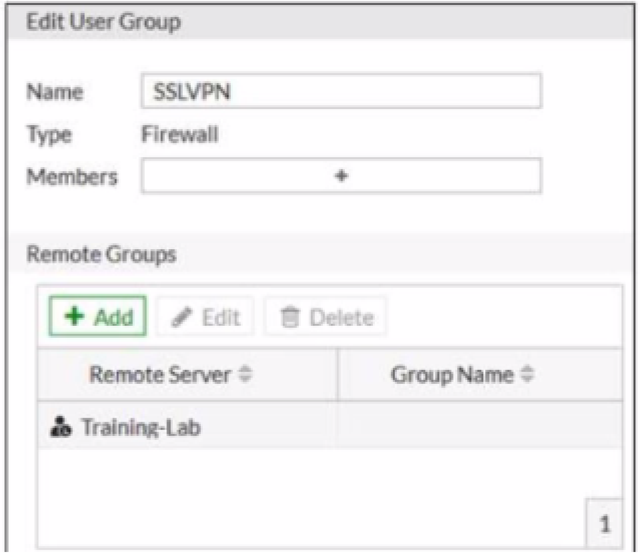
Explanation:

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.

Question 12

Question Type: MultipleChoice

Refer to the exhibit.



Edit User Group

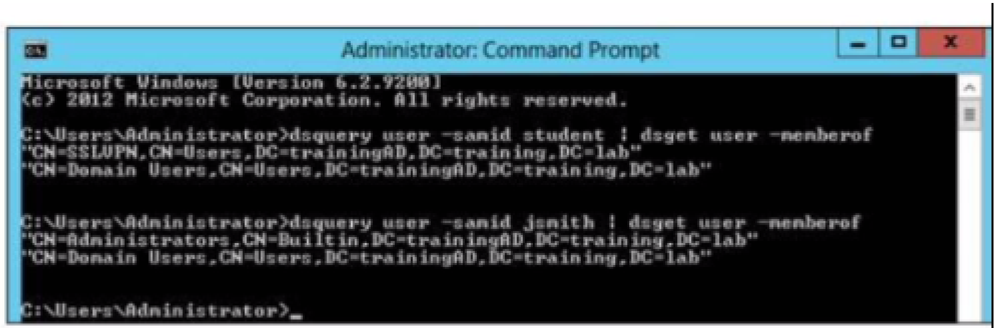
Name: SSLVPN

Type: Firewall

Members:

Remote Groups

Remote Server	Group Name
Training-Lab	



Administrator: Command Prompt

```
Microsoft Windows [Version 6.2.9200]
(c) 2012 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>dsquery user -samid student | dsget user -memberof
"CN=SSLVPN,CN=Users,DC=trainingAD,DC=training,DC=lab"
"CN=Domain Users,CN=Users,DC=trainingAD,DC=training,DC=lab"


C:\Users\Administrator>dsquery user -samid jsmith | dsget user -memberof
"CN=Administrators,CN=Builtin,DC=trainingAD,DC=training,DC=lab"
"CN=Domain Users,CN=Users,DC=trainingAD,DC=training,DC=lab"


C:\Users\Administrator>_
```

Examine the FortiGate user group configuration and the Windows AD LDAP group membership information shown in the exhibit

FortiGate is configured to authenticate SSL VPN users against Windows AD using LDAP The administrator configured the SSL VPN user group for SSL VPN users However the administrator noticed that both the student and j smith users can connect to SSL VPN

Which change can the administrator make on FortiGate to restrict the SSL VPN service to the student user only?

Options:

A- In the SSL VPN user group configuration set Group Nam to CN-SSLVPN, CN='users, DC-trainingAD, DC-training, DC-lab

B- In the SSL VPN user group configuration, change Name to cn=sslvpn, CN=users, DC=trainingAD, Detraining, DC-lab.

C- In the SSL VPN user group configuration set Group Name to ::;=Domain users.CN-Users/DC=trainingAD, DC-training, DC=lab.

D- In the SSL VPN user group configuration change Type to Fortinet Single Sign-On (FSSO)

Answer:

A

Explanation:

According to the FortiGate Administration Guide, "The Group Name is the name of the LDAP group that you want to use for authentication. The name must match exactly the name of the LDAP group on the LDAP server." Therefore, option A is true because it will set the Group Name to match the LDAP group that contains only the student user. Option B is false because changing the Name will not affect the authentication process, as it is only a local identifier for the user group on FortiGate. Option C is false because setting the Group Name to Domain Users will include all users in the domain, not just the student user. Option D is false because changing the Type to FSSO will require a different configuration method and will not solve the problem.