HPE6-A48 Q&As

Aruba Certified Mobility Expert 8 Written Exam

Pass HP HPE6-A48 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.certbus.com/hpe6-a48.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by HP Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

A foreign exchange broker in a shared office space uses an Aruba Mobility Master (MM)-Mobility Controller (MC) architecture along with ClearPass and AirWave. The corporate network is FXBroker121, but users report that they cannot access the FXBroker111 SSID. The team suspects that a rogue AP is in place and a malicious user tried to disguise the WLAN name.

How can the organization\\'s network administrator identify and locate the potential rogue AP?

A. Create an AirWave RAPIDS rule with a Suspected Rogue classification and the SSID Matches FXBroker111 condition, then access any RAPID List entry that matches the rule and click on Location.

B. Use ClearPass Event viewer and search for entries with the FXBroker111 Aruba-Essid-Name VSA attribute, then obtain the value of the Aruba-AP-Group attribute.

C. Use ClearPass Event viewer and search for entries with the FXBroker111 Aruba-Essid-Name VSA attribute, then obtain the value of the Aruba-Location-id attribute.

D. Create and AirWave RAPIDS rule with a Suspected Rogue classification and the SSID Does Not Match FXBroker121 condition, then access any RAPIDS List entry that matches the rule and click on Location.

Correct Answer: B

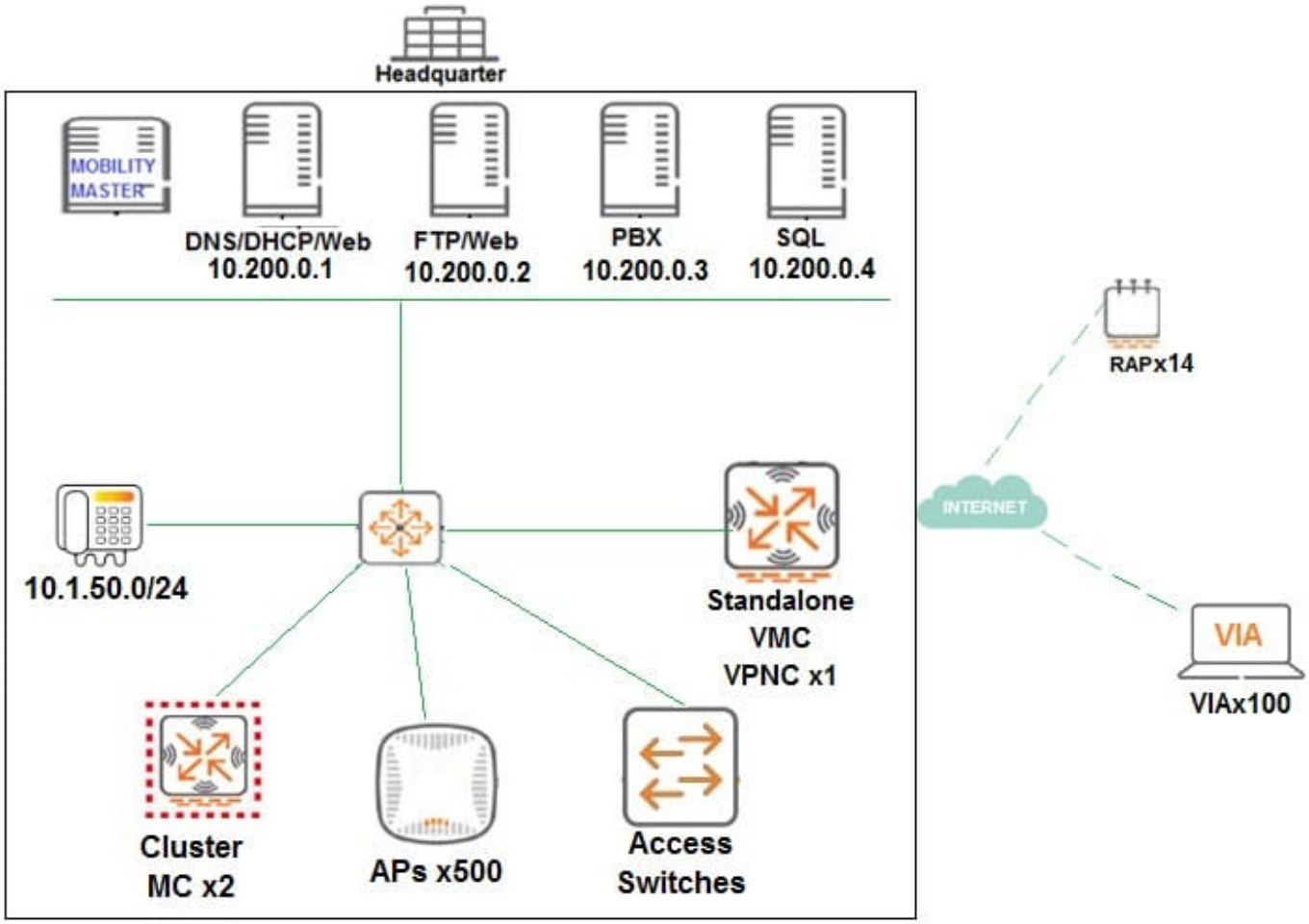
QUESTION 2

A financial institution contacts an Aruba partner to deploy an advanced and secure Mobility Master (MM)Mobility Controller (MC) WLAN solution in its main campus and 14 small offices/home offices (SOHOs). Key requirements are that users at all locations, including telecommuters with VIA, should be assigned roles with policies that filter undesired traffic. Also, advanced WIPs should be enforced at the campus only.

These are additional requirements for this deployment:

RAPs should ship directly to their final destinations without any pre-setup and should come up with the right configuration as soon as they get Internet access. Activate should be configured with devices MACs, serial numbers, and provisioning rules that redirect them to the standalone VMC at the DMZ Users should be able to reach DNS, FTP, Web and telephone servers in the campus as well as send and receive IP telephone calls to and from the voice 10.1.50.0/24 segment. Local Internet access should be granted.

Refer to the exhibit.



Refer to the scenario and the exhibit.

```
(MC2) [MDC] #show ip access-list split-tunneling

ip access-list session split-tunneling
split-tunnelimg
----------
Priority  Source                Destination                Service     Application  Action  TimeRange
--------  ------                -----------                -------     -----------  ------  ---------
1         any                   any                        svc-dhcp                 permit

Log  Expired  Queue  TOS  8021P  Blacklist  Mirror  Dis  Scan  IPv4/6
---  -------  -----  ---  -----  ---------  ------  ---  ----  -------
                Low                                             4
2          user                 10.200.0.0.255.255.255.252  any          permit

                Low                                             4
3       10.200.0.0 255.255.255.252  user                   any          permit

                Low                                             4
4          user                 10.1.50.0 255.255.255.0    svc-rtsp     permit

                Low                                             4
5          user                 10.1.50.0 255.255.255.0    svc-sip-udp  permit

                Low                                             4
6          10.1.50.0 255.255.255.0  user                   svc-rtsp     permit

                Low                                             4
7          10.1.50.0 255.255.255.0  user                   svc-sip-udp  permit

                Low                                             4
```

Which command must the network administrator add in the split-tunneling policy to meet the requirements for the RAP employee SSID?

A. user any svc-http permit

B. user any any src-nat pool dynamic-srcnat

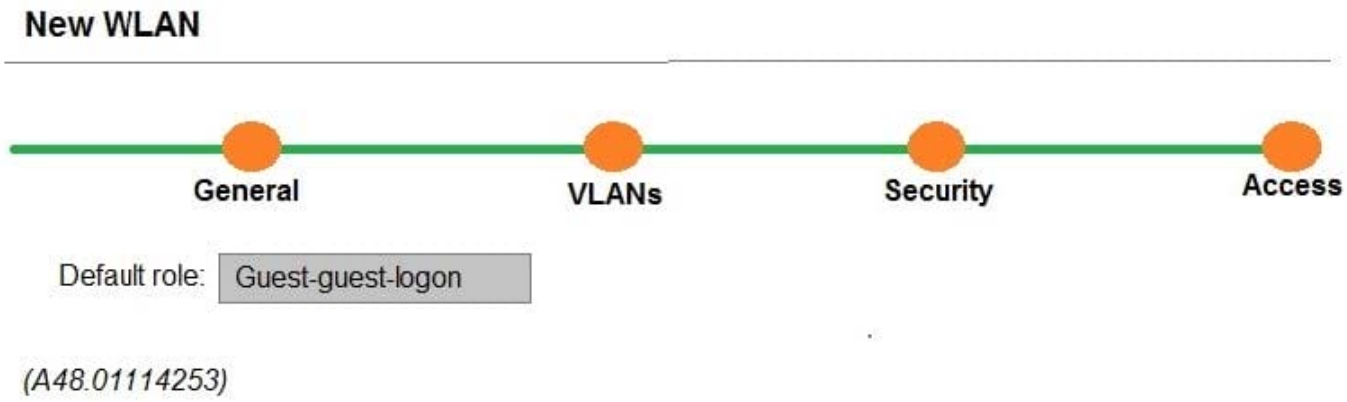
C. any user any src-nat pool dynamic-srcnat

D. user any any dst-nat

Correct Answer: B

QUESTION 3

Refer to the exhibit.



A network administrator completes the task to cretae a WLAN, as shown in the exhibit. The network administrator selects the options to use guest as primary usage and Internal captive portal with authentication in the security step. Next, the network administrator creates a policy that denies access to the internal network.

Which additional step must the network administrator complete in order to prevent authenticated users from reaching internal corporate resources while allowing Internet access?

A. Apply the policy on the guest-guest-logon role.

B. Apply the policy on the authenticated role.

C. Apply the policy on the guest role.

D. Create a policy that permits dhcp, dns, and http access.

Correct Answer: D

QUESTION 4

Refer to the exhibit.

```
(MM1) [mynode] #show ip interface brief

Interface     IP Address   /  IP Netmask      Admin     Protocol     VRRP-IP
vlan 1        10.254.10.14 /  255.255.255.0  up        up           10.254.10.214
loopback      unassigned   /  unassigned     up        up
mgmt          unassigned   /  unassigned     down      down
(MM1) [mynode] #show vrrp

Virtual Router 140:
        Description MM1
        Admin State UP, VR State BACKUP
        IP Address 10.254.10.214, MAC Address 00:00:5e:00:01:8c, vlan1
        Priority 100, Advertisement 5 sec, Preemption Enable Delay 60
        Auth type PASSWORD, Auth data: ********
        tracking is not enabled
(MM1)  [mynode]#
```

After a recent power outage where MM1 is located, the network administrator could not perform configuration tasks on Mobility Controllers (MC) for several hours. The network administrator decides to acquire another Mobility Master (MM) and deploy L2 MM redundancy. The new MM is assigned the

10.254.10.15 IP address and VRRP is configured in both units. The network administrator verifies that VRRP is running, and prepares to complete the setup with the following scripts.

```
/mm/mynode (MM1):
     master-redundancy
     master-vrrp 140
     peer-ip-address 10.254.10.15 ipsec key123
/mm/mynode (MM2):
     master-redundancy
     master-vrrp 140
     peer-ip-address 10.254.10.14 ipsec key123

/mm (MM1):
database synchronize period 30
```

Which configuration tasks must the network administrator do before applying the script in order to successfully deploy L2 MM redundancy and prevent any other control plane outage?

A. Confirm that the VRRP and master redundancy keys are the same.

B. Change the VIP address of ther VRRP process 140 to 10.254.10.15.

C. Reduce the VRRP priority to 90 and restart the process in MM2.

D. Enable the MM database synchronization in MM2.

Correct Answer: A

QUESTION 5

A point venture between two companies results in a fully functional WLAN Aruba solution. The network administrator uses the following script to integrate the WLAN solution with two radius servers, radius1 and radius2.

```
aaa athentication-server radius radius1
  host 10.254.1.1
  key key111
!
aaa authentication-server radius radius2
  host 10.20.2.2
  key key222
!
aaa server-group group-corp
auth-server radius1

aaa profile aaa-corp
authentication-dot1x authenticated
dot1x-server-group group-corp
!
wlan ssid-profile ssid-corp
essid corp
opmode wpa2-aes
!
wlan virtual-ap vap-corp
aaa-profile aaa-corp
ssid-profile ssid-corp
!
ap-group building1
virtual-ap vap-corp
```

While all users authenticate with username@doaminname.com type of credentials, radius1 has user accounts without the domain name portion.

Which additional configuration is required to authenticate corp1.com users with radius1 and corp2 users with radius2?

A. aaa authentication-server radius radius1 trim-fqdn ! aaa server-group-corp auth-server radius1 match-authstring corp1.com auth-server radius1 match-authstring corp2.com

B. aaa server-group-corp auth-server radius1 match-fqdn corp1.com auth-server radius1 trim-fqdn auth-server radius2 match-fqdn corp2.com

C. aaa authentication-server tadius radius1 ! aaa server-group-corp auth-server radius1 match-string corp1.com trim-fqdn auth-server radius1 match-string corp2.com

D. aaa authentication-server radius radius1 trim-fqdn ! aaa server-group-corp auth-server radius1 match-domain corp1.com auth-server radius1 match-domain corp2.com

Correct Answer: B

QUESTION 6

Refer to the exhibit.

```
(MC2) #show auth-tracebuf mac 70:4d:7b:10:9e:c6 count 27
Warning: user-debug is enabled on one or more specific MAC addresses:
         only those MAC addresses appear in the trace buffer.

Auth Trace Buffer
-----------------------------
Jun 29 20:56:51  station-up      *   70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0              - -     wpa2 aes
Jun 29 20:56:51  eap-id-req      <-  70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0              1 5
Jun 29 20:56:51  eap-start      ->  70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0              - -
Jun 29 20:56:51  eap-id-req      <-  70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0              1 5
Jun 29 20:56:51  eap-id-resp     ->  70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0              1 7     it
Jun 29 20:56:51  rad-req         ->  70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0              42 174  10.1.140.101
Jun 29 20:56:51  eap-id-resp     ->  70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0              1 7     it
Jun 29 20:56:51  rad-resp        <-  70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0/RADIUS1      42 88
Jun 29 20:56:51  eap-req         <-  70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0              2 6
Jun 29 20:56:51  eap-resp        ->  70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0              2 214
Jun 29 20:56:51  rad-req         ->  70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0/RADIUS1      43 423  10.1.140.101
Jun 29 20:56:51  rad-resp        <-  70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0/RADIUS1      43 228
Jun 29 20:56:51  eap-req         <-  70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0              3 146
Jun 29 20:56:51  eap-resp        ->  70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0              3 61
Jun 29 20:56:51  rad-req         ->  70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0/RADIUS1      44 270  10.1.140.101
Jun 29 20:56:51  rad-resp        <-  70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0/RADIUS1      44 128
Jun 29 20:56:51  eap-req         <-  70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0              4 46
Jun 29 20:56:51  eap-resp        ->  70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0              4 46
Jun 29 20:56:51  rad-req         ->  70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0/RADIUS1      45 255  10.1.140.101
Jun 29 20:56:51  rad-accept      <-  70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0/RADIUS1      45 231
Jun 29 20:56:51  eap-success     <-  70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0              4 4
Jun 29 20:56:51 user repkey change *70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0          65535 -   204c0306e790000000170008
Jun 29 20:56:51 macuser repkey change * 70:4d:7b:10:9e:c6  70:3a:0e:5b:0a:c0     65535 - 70:4d:7b:10:9e:c6
Jun 29 20:56:51  wpa2-key1      <-  70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0              -   117
Jun 29 20:56:51  wpa2-key2      ->  70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0              -   117
Jun 29 20:56:51  wpa2-key3      <-  70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0              -   151
Jun 29 20:56:51  wpa2-key4      ->  70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0              -   95
```

A network administrator is validating client connectivity and executes the show command shown in the exhibit. Which authentication method was used by the wireless station?

A. 802.1X user authentication

B. EAP authentication

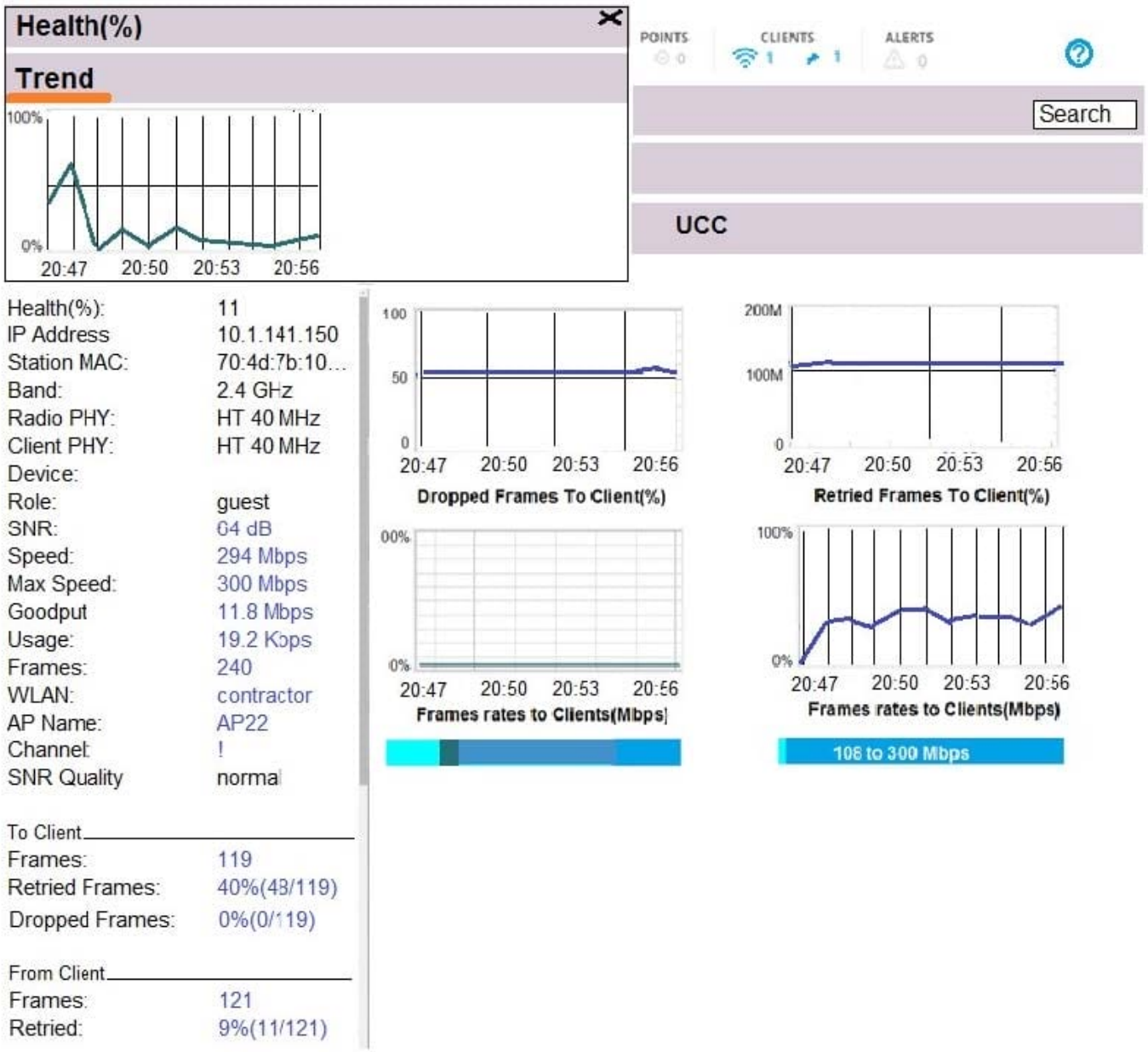
C. 802.1X machine authentication

D. MAC authentication

Correct Answer: C

QUESTION 7

Refer to the exhibit.



A user\\'s laptop only operates in the 2.4 GHz band and supports 802.11n. This user reports that the network is slow at the cafeteria that is serviced by three APs, and suggests that there might be a problem with the WLAN. The network administrator finds the user in the MM, and obrains the output shown in the exhibit.

What should the network administrator do to optimize the client connection?

A. Disable lower transmit rates in the SSID profile.

B. Change the channel being used in the radio profile.

C. Reduce Min/Max channel bandwidth in the radio profile.

D. Reduce Min/Max EIRP in the ARM profile.

Correct Answer: A

QUESTION 8

A customer with a multi-controller network upgrades the ArubaOS from 6.4 to 8. The customer\\'s clients must be able to move between different locations of the campus without disconnecting their applications, when roaming or if there are Mobility Controller (MC) failures. The customer also wants to have full control of the users, and be able to change their session properties from a RADIUS server.

Which steps must the network consultant include in the implementation plan to meet these requirements?

A. 1. Create a controller cluster profile that contains the management and VRRP IP addresses of each member.

2.

Apply the profile to all MCs in the cluster.

3.

Confirm that the cluster is L2 connected.

B. 1. Configure a VRRP instance for all MCs

2.

Create a controller cluster profile that contains the management IP and VIP addresses of each MC.

3.

Apply the profile to all MCs in the cluster.

4.

Confirm that the cluster is L2 connected.

C. 1. Configure a VRRP instance for each MC.

2.

Create a controller cluster profile that contains the management IP of each member.

3.

Apply the profile to all MCs in the cluster.

4.

Confirm that the cluster is L3 connected.

D. 1. Create a controller cluster profile that contains the management and VRRP IP addresses of each member.

2.

Apply the profile to the cluster leader.

3.

Confirm that the cluster is L2 connected.

Correct Answer: D

QUESTION 9

Refer to the exhibit.

```
a8:bd:27:c5:c3:3a# sh dhcp subnets

DHCP Subnet Table
-------------------------------
VLAN  Type  Subnet        Mask             Gateway      Mode                 Rolemap
----- ----- ------------- ---------------- ------------ -------------------- ------------
124   l3    10.21.124.32  255.255.255.224  10.21.124.33 local,split-tunnel
81    l2    0.0.0.0       255.255.255.255  0.0.0.0      remote,full-tunnel
```

A network engineer deploys two different DHCP pools in an Instant AP (IAP) cluster for WLANs that will have connectivity to a remote site using Aruba IPSec.

Based on the output shown in the exhibit, which IAP-VPN DHCP modes are being used?

A. distributed L3 and centralized L3

B. distributed L3 and local L3

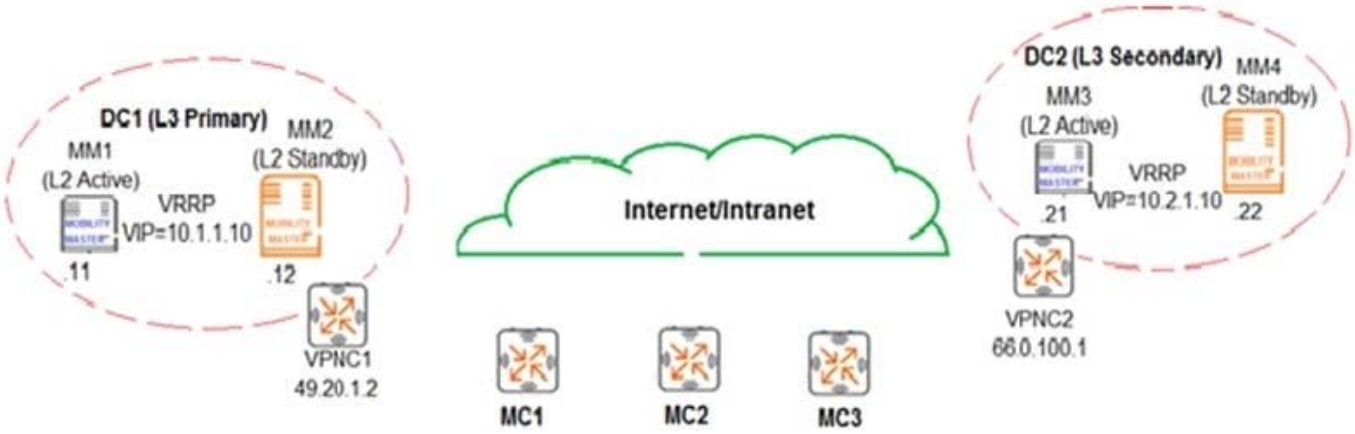
C. distributed L3 and centralized L2

D. local L3 and centralized L2

Correct Answer: C

QUESTION 10

Refer to the exhibit.



An Aruba network is deployed with L2 and L3 Mobility Master (MM) redundancy across two datacenters, as shown in the exhibit. The network administrator confirms that all Mobility Controllers (MC) are currently communicating with MM1, which is the L2 Active, and L3 Primary. Which MM IP will MCs communicate with if MM1 fails?

A. 10.1.1.10

B. 10.1.1.12

C. 10.2.1.10

D. 10.2.1.21

Correct Answer: B

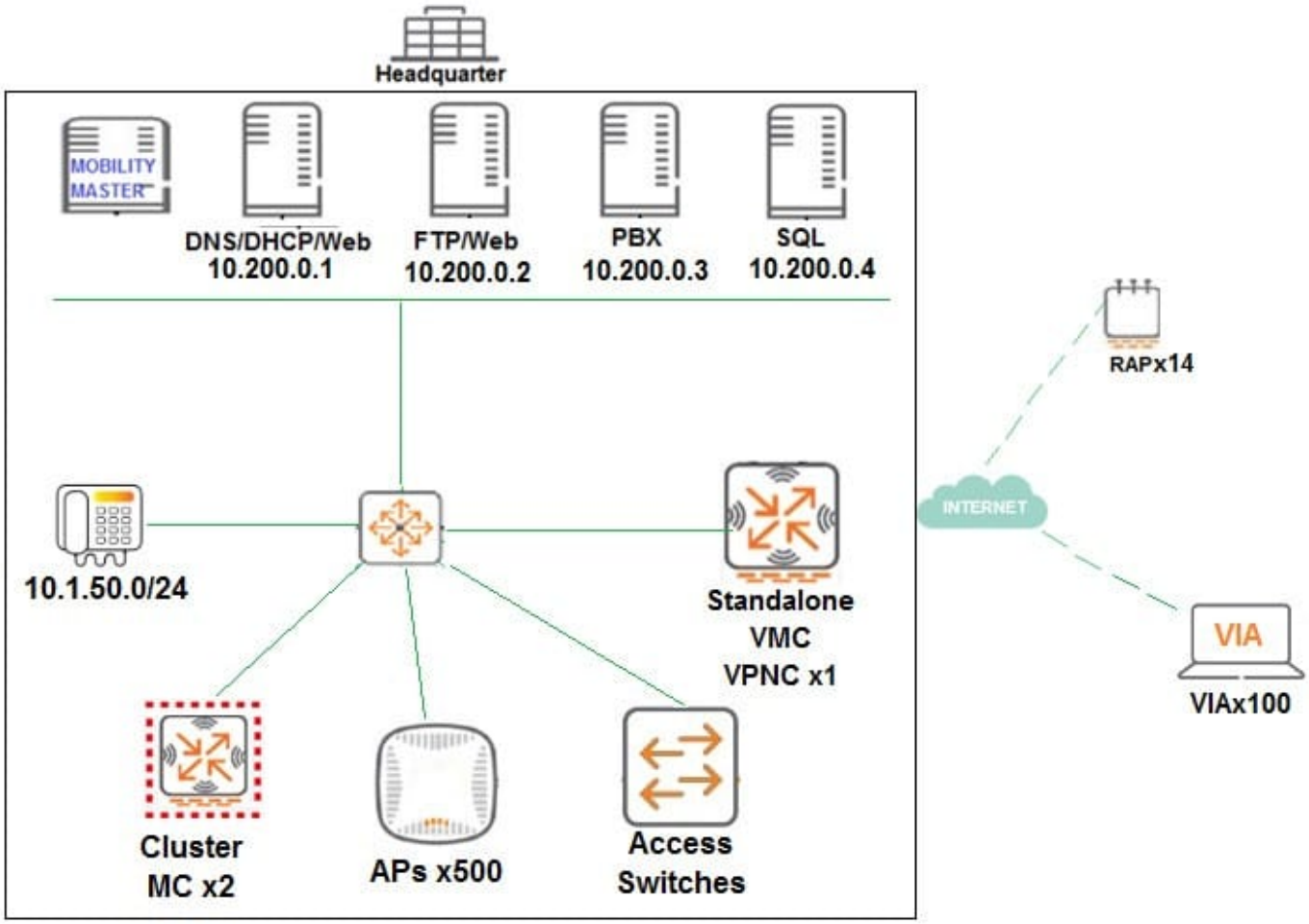
QUESTION 11

A financial institution contacts an Aruba partner to deploy an advanced and secure Mobility Master (MM)Mobility Controller (MC) WLAN solution in its main campus and 14 small offices/home offices (SOHOs). Key requirements are that users at all locations, including telecommuters with VIA, should be assigned roles with policies that filter undesired traffic. Also, advanced WIPs should be enforced at the campus only.

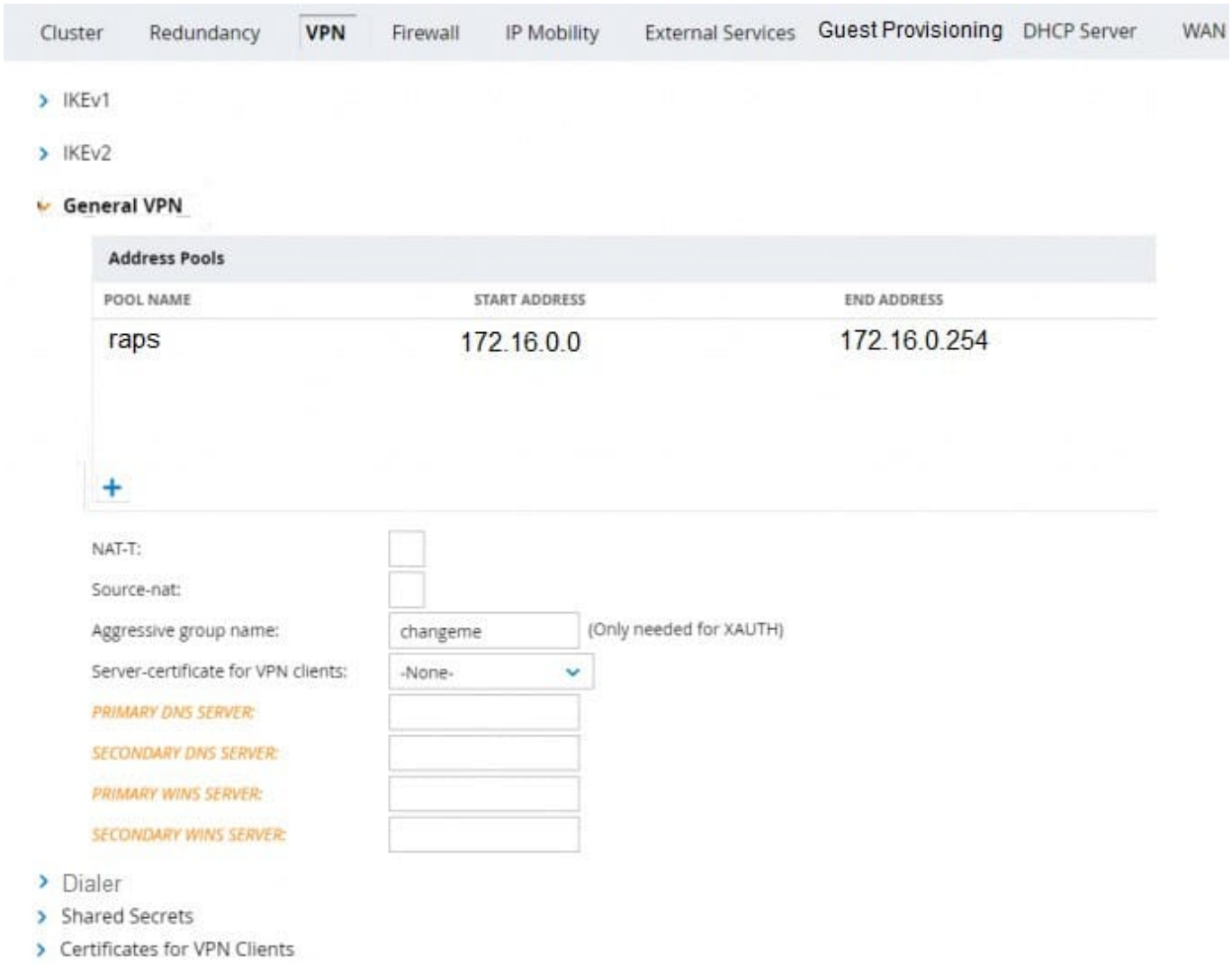
These are additional requirements for this deployment:

RAPs should ship directly to their final destinations without any pre-setup and should come up with the right configuration as soon as they get Internet access. Activate should be configured with devices MACs, serial numbers, and provisioning rules that redirect them to the standalone VMC at the DMZ Users should be able to reach DNS, FTP, Web and telephone servers in the campus as well as send and receive IP telephone calls to and from the voice 10.1.50.0/24 segment. Local Internet access should be granted.

Refer to the exhibit.



Refer to the scenario and the exhibit.



The standalone VMC will act as a VPN Concentrator of the RAPs. The network administrator configures the Standalone VMC with a pool of addresses and the SOHOs AP Group from the MM.

Which additional steps must the network administrator perform to allow the RAPs to terminate their IPSec tunnels and associate to the Standalone VMC?

A. Add RAP MAC addresses into the RAP whitelist, and associate them with the SOHOs AP-Group.

B. Add RAP MAC addresses into the CPSec whitelist, and associate them with the SOHOs AP-Group.

C. Configure the same IP Pool at the MM group level, then create user accounts for the RAPs in the internal database.

D. Create user accounts with the sys-ap-role, and define shared secrets to associate to RAP IP addresses at the MM group level.

Correct Answer: D

QUESTION 12

A company has headquarters based in the US and rents internation office space in Mexico City so that 10 employees can work remotely. The company must implement a remote access technology so branch office employees can access all servers at the headquareters.

The office has both wired and wireless internet connectivity, with no restrictions on what device connects to the network. However, ports UDP 4500, 5060, and 5061 are blocked by the primeter firewall.

Which remote access technology is required to allow employees to access the servers at the headquarters?

A. BOC with CAPs

B. IAP VPN

C. RAP

D. VIA

Correct Answer: C

QUESTION 13

Refer to the exhibit.

```
(MM1) [mynode] #show airmatch debug history ap-name AP20

2 GHz radio mac 70:3a:0e:5b:0a:c0   ap name  AP20
```

Time of Change	Chan	Bandwidth	EIRP(dBm)	Mode	Source
2018-07-16 05:01:56	11->11	20-> 20	8.0-> 23.0	AP->AP	Solver
2018-07-16 05:01:48	6 ->11	20-> 20	8.0-> 8.0	AP ->AP	Solver
2018-07-15 13:26:13	11 -> 7	20-> 40	8.0-> 6.0	AP ->AP	Min Channel Bandwidth Change
2018-07-15 12:21:39	1 ->11	40-> 20	8.0-> 6.0	AP ->AP	Max Channel Bandwidth Change
2018-07-15 12:20:08	11 -> 1	20-> 40	8.0-> 6.0	AP ->AP	Min Channel Bandwidth Change
2018-07-15 12:18:47	7 ->11	40-> 20	8.0-> 6.0	AP ->AP	Max Channel Bandwidth Change
2018-07-15 11:47:26	11-> 7	20-> 40	8.0-> 6.0	AP ->AP	Min Channel Bandwidth Change

Help desk staff receive reports from users that there is inefficient wireless service in a location serviced by AP20, AP21, and AP22, and open a ticket. A few hours later, the users report that there is a drastic improvement in service. The staff still wants to determine the cause of the problem so the next day thay start monitoring the tasks.

They access the Mobility Master (MM), and obtain the output shown in the exhibit.

What could be the cause of the problem that the users reported?

A. AirMatch was running an initial incremental optimization.

B. An operator used AirMatch to manually freeze AP channel and power.

C. An operator manually assigned settings in the radio profile.

D. AirMatch was running a full on-demand optimization.

Correct Answer: B

QUESTION 14

A bank deploys an Aruba Mobility Master (MM)-Mobility Controller (MC) solution to provide wireless access for users that run different applications on their laptops, including SIP-based IP telephony. When users only run the IP telephony software, call quality is high. However, if users also run email, web, or mission critical applications, then voice quality drops.

Which feature would help improve the quality of voice calls over the air when users run different applications?

A. DSCP for IPv4 traffic

B. WiFi Multi Media

C. Type of Service

D. High/Low Queue

Correct Answer: A

QUESTION 15

A network administrator assists with the migration of a WLAN from a third-party vendor to Aruba in different locations throughout the country. In order to manage the solution from a central point, the network administrator decides to deploy redundant Mobility Masters (MMs) in a datacenter that are reachable through the Internet.

Since not all locations own public IP addresses, the security team is not able to configure strict firewall policies at the datacenter without disrupting some MM to Mobility Controller (MC) communications. They are also concerned about exposing the MMs to unauthorized inbound connection attempts.

What should the network administrator do to ensure the solution is functional and secure?

A. Deploy an MC at the datacenter as a VPN concentrator.

B. Block all ports to the MMs except UDP 500 and 4500.

C. Install a PEFV license, and configure firewall policies that protect the MM.

D. Block all inbound connections, and instruct the MM to initiate the connection to the MCs.

Correct Answer: C