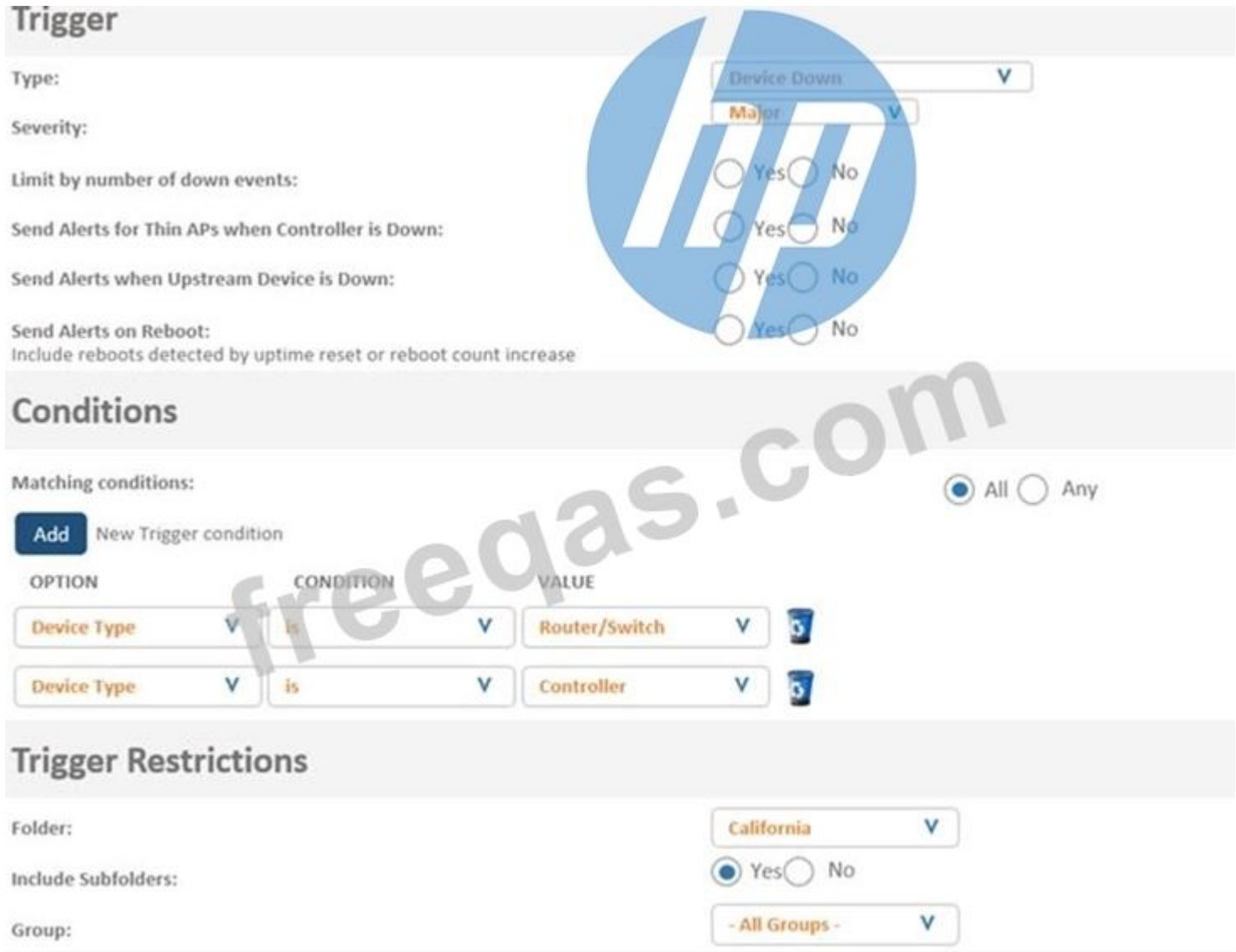
HP.HPE6-A79.v2022-04-06.q19

Exam Code:	HPE6-A79
Exam Name:	Aruba Certified Mobility Expert Written Exam
Certification Provider:	HP
Free Question Number:	19
Version:	v2022-04-06
# of views:	668
# of Questions views:	190
https://www.freeqas.com/qa/HP/HPE6-A79/HP.HPE6-A79.v2022-04-06.q19.html	

NEW QUESTION: 1
An organization owns a fully functional multi-controller Aruba network with a Virtual Mobility Master (VMM) in VLAN20. They have asked a network consultant to deploy a redundant MM on a different server. The solution must offer the lowest convergence time and require no human interaction in case of failure.
The servers host other virtual machines and are connected to different switches that implement ACLs to protect them. The organization grants the network consultant access to the servers only, and appoints a network administrator to assist with the deployment.
What must the network administrator do so the network consultant can successfully deploy the solution? (Choose two.)
A. Configure an ACL entry that permits IP protocol 50, UDP port 500, and multicast IP 224.0.0.18.
B. Allocate VLAN20 to the second server, and extend it throughout the switches, then reserve one IP address for the second MM and another for the VIP.
C. Allocate VLAN20 to the second server, and permit routing between them, then reserve one IP address for the second MM and another IP address for its gateway.
D. Configure an ACL entry that permits UDP 500, TCP 4500, and multicast IP 224.0.0.5.
E. Allocate VLAN20 to the second server, and extend it throughout the switches, then reserve one IP address for the second MM and another IP address for its gateway.
Answer: D,E (LEAVE A REPLY)

NEW QUESTION: 2
A network administrator wants to receive a major alarm every time a controller or an Aruba switch goes down for either a local or an upstream device failure. Which alarm definition must the network administrator create to accomplish this?



Answer:

NEW QUESTION: 3
Refer to the exhibit.

```
(MM)[mynode] #show airmatch event all-events ap-name AP2

Band  Event Type    Radio              Timestamp           Chan       CBW        New Chan   New CBW    APName
----  ----------    -----------------  ------------------  ---------  ---------  ---------  ---------  ---------
5GHz  RADAR_DETECT  xx:xx:xx:xx:xx:xx  2018-07-25_07:50:05      100      80MHz        149      80MHz  AP2
5GHz  NOISE_DETECT  xx:xx:xx:xx:xx:xx  2018-07-24_07:48:42      124      80MHz        100      80MHz  AP2
5GHz  RADAR_DETECT  xx:xx:xx:xx:xx:xx  2018-07-23_16:44:36      100      80MHz        124      80MHz  AP2
5GHz  NOISE_DETECT  xx:xx:xx:xx:xx:xx  2018-07-20_19:12:34      157      80MHz        100      80MHz  AP2
5GHz  RADAR_DETECT  xx:xx:xx:xx:xx:xx  2018-07-20_10:02:30      100      80MHz        157      80MHz  AP2
5GHz  RADAR_DETECT  xx:xx:xx:xx:xx:xx  2018-07-20_08:34:31       56      80MHz        100      80MHz  AP2

2GHz  NOISE_DETECT  xx:xx:xx:xx:xx:xx  2018-07-25_08:31:31       11      20MHz          6      20MHz  AP2
2GHz  NOISE_DETECT  xx:xx:xx:xx:xx:xx  2018-07-25_08:31:31        6      20MHz          1      20MHz  AP2
2GHz  NOISE_DETECT  xx:xx:xx:xx:xx:xx  2018-07-24_07:46:34        1      20MHz         11      20MHz  AP2
2GHz  NOISE_DETECT  xx:xx:xx:xx:xx:xx  2018-07-24_07:46:33        6      20MHz          1      20MHz  AP2
2GHz  NOISE_DETECT  xx:xx:xx:xx:xx:xx  2018-07-23_15:13:15       11      20MHz          6      20MHz  AP2
2GHz  NOISE_DETECT  xx:xx:xx:xx:xx:xx  2018-07-23_15:12:12        1      20MHz         11      20MHz  AP2
2GHz  NOISE_DETECT  xx:xx:xx:xx:xx:xx  2018-07-20_08:07:27       11      20MHz          1      20MHz  AP2
2GHz  NOISE_DETECT  xx:xx:xx:xx:xx:xx  2018-07-20_08:07:26        6      20MHz         11      20MHz  AP2
2GHz  NOISE_DETECT  xx:xx:xx:xx:xx:xx  2018-07-19_19:22:45        1      20MHz          6      20MHz  AP2
2GHz  NOISE_DETECT  xx:xx:xx:xx:xx:xx  2018-07-19_19:22:44       11      20MHz          1      20MHz  AP2
2GHz  NOISE_DETECT  xx:xx:xx:xx:xx:xx  2018-07-19_10:45:23        1      20MHz         11      20MHz  AP2
```

A network administrator deploys a Mobility Master (MM) - Mobility Controller (MC) network with Aps in different locations. Users in one of the locations report that the WiFi network works fine for several hours, and then they are suddenly disconnected. This symptom may happen at any time, up to three times every day, and lasts no more than two minutes.

After some research, the network administrator logs into the MM and reviews the output shown in the exhibit.

Based on this information, what is the most likely reason users get disconnected?

A. AirMatch is reacting to non-scheduled RF events.

B. Users in the 2.4 GHz band are being affected by high interference.

C. AirMatch is applying a scheduled optimization solution.

D. Adaptive Radio Management is reacting to RF events.

Answer: (SHOW ANSWER)

NEW QUESTION: 4

Refer to the exhibit.

A network administrator wants to configure an 802.1x supplicant for a wireless network that includes the following:

* AES encryption
* EAP-MSCHAP v2-based user and machine authentication
* Validation of server certificate in Microsoft Windows 10

The network administrator creates a WLAN profile and selects the change connection settings option. Then the network administrator changes the security type to Microsoft: Protected EAP (PEAP), and enables user and machine authentication under Additional Settings.

What must the network administrator do next to accomplish the task?

A. Enable user authentication under Settings

B. Change default RC4 encryption for AES.

C. Change the security type to Microsoft: Smart Card or other certificate.

D. Enable server certificate validation under Settings.

Answer: (SHOW ANSWER)

NEW QUESTION: 5

Refer to the exhibit.

```
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_request.c:67] Add Request: id=45, server=ClearPass, IP=10.254.1.23, server-group=Employee,
 fd=63
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:2367] Sending radius request to ClearPass:10.254.1.23:1812 id:45, len:260
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:2383]  User-Name: contractor12
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:2383]  NAS-IP-Address: 10.254.13.14
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:2383]  NAS-Port-Id: 0
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:2383]  NAS-Identifier: 10.254.13.14
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:2383]  NAS-Port-Type: Wireless-IEEE802.11
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:2383]  Calling-Station-Id: 608E9A910FT8
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:2383]  Called-Station-Id: 446468O7DE4G
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:2383]  Service-Type: Framed User
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:2383]  Framed MTU: 1100
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:2383]  EAP-Message: \002\012
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:2383]  State: AGcATgBnAKj9IQQAkgYQj1ulavmnP5/OVnaOPQ==
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:2383]  Aruba-Essid-Name: EmployeesNet
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:2383]  Aruba-Location-Id: AP22
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:2383]  Aruba-AP-Group: CAMPUS
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:2381]  Aruba-Device-Type: (VSA with invalid length - Don't send it)
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:2383]  Message-Auth:  487e\326\445\540\318/f\789\416\110\874\4482\612
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:95]  Find Request: id=45, server=(null), IP=10.254.1.23, server-group=(null) fd=63
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:104] Current entry: server=(null), IP=10.254.1.23, server-group=(null), fd=63
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:48]  Del Request: id=45, server=ClearPass, IP=10.254.1.23, server-group=Employee,
fd=63
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:1228] Authentication Successful
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:1230] RADIUS RESPONSE ATTRIBUTES:
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:1245]  {Aruba} Aruba-User-Role: contractor
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:1245]  {Microsoft} MS-MPPE-Recv-Key: \640\510\973>J\644\238n\421\789\252iP\612\439|K
\0551\898h\354\519\733Fe0\450\739(\456\152="c\217bR\794\777\649\147\682\400\118\493y\452\731(
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:1245]  {Microsoft} MS-MPPE-Send-Key: \641\486\489\011\605\784\064h\027\3824\677\723\
884 \375o\446 \398\453
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:1245]  EAP-Message: \003\012
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:1245]  Message-Auth: z\498XS\330\480\512\383\498\711
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:1245]  User-Name: contractor12
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:1245]  Class: \202\005\456)\123\789C\056\2578#\876\041\579"\656\741\081
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:1245]  PW_RADIUS_ID: -
Jun 23 21:28:17 :121031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:1245]  Rad-Length: 250
Jun 23 21:28:17 :124031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:1245]  PW_RADIUS_CODE: \002
Jun 23 21:28:17 :124031:  <5533> <DBUG> |authmgr| |aaa| [rc_server.c:1245]  PW_RAD_AUTHENTICATOR: PN\495\591\685$\211\481\982G\363RD\261\696\025
Jun 23 21:28:17 :124003:  <5533> <INFO> |authmgr| Authentication result= Authentication Successful(0), method=802.1x, server=ClearPass, user=xx:xx:xx:
xx:xx:xx
```

A network administrator wants to allow contractors to access the WLAN named EmployeesNet. In order to restrict network access, the network administrator wants to assign this category of users to the contractor user role. To do this, the network administrator configures ClearPass in a way that it returns the Aruba-User-Role with the contractor value.

When testing the solution, the network administrator receives the wrong role.

What should the network administrator do to assign the contractor role to contractor users without affecting any other role assignment?

A. Set contractor as the default role in the AAA profile.

B. Check the Download role from the CPPM option in the AAA profile.

C. Create server deviation rules in the server group.

D. Create Contractor firewall role in the M.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 6

Refer to the exhibits.

1 Controller

3 Access Devices

Access Points 3 filtered by Status **Up**

	NAME	STATUS	CLIENTS	UPTIME	MANAGED ...	GROUP	MODEL
>	AP-Upper_Level	Up	4	1w 3d	MC_VA	Haras	205
>	AP-Lower_Level	Up	2	1w 3d	MC_VA	Haras	303H
v	AP-Garden	Up	10	1w 3d	MC_VA	Haras	365

DETAILS

Name
AP-Garden

IP address
172.32.0.25

MAC address
44:48:c1:ca:7e:6a

AP group
Haras

Model
365

Managed by
MC_VA

Operating mode
Remote

WLANs
5

Connected clients
10

To clients
11.3 Mbps

From clients
10.1 Mbps

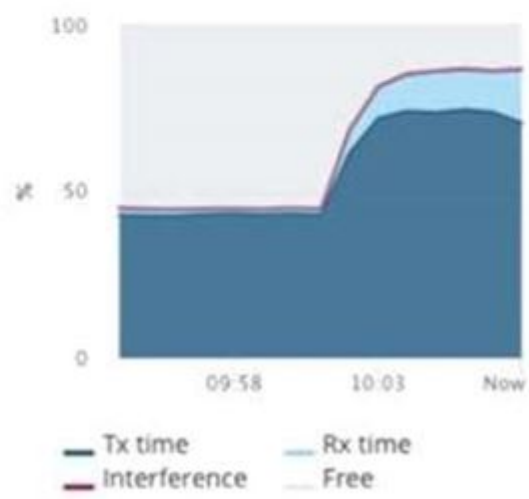
Provisioned
Yes

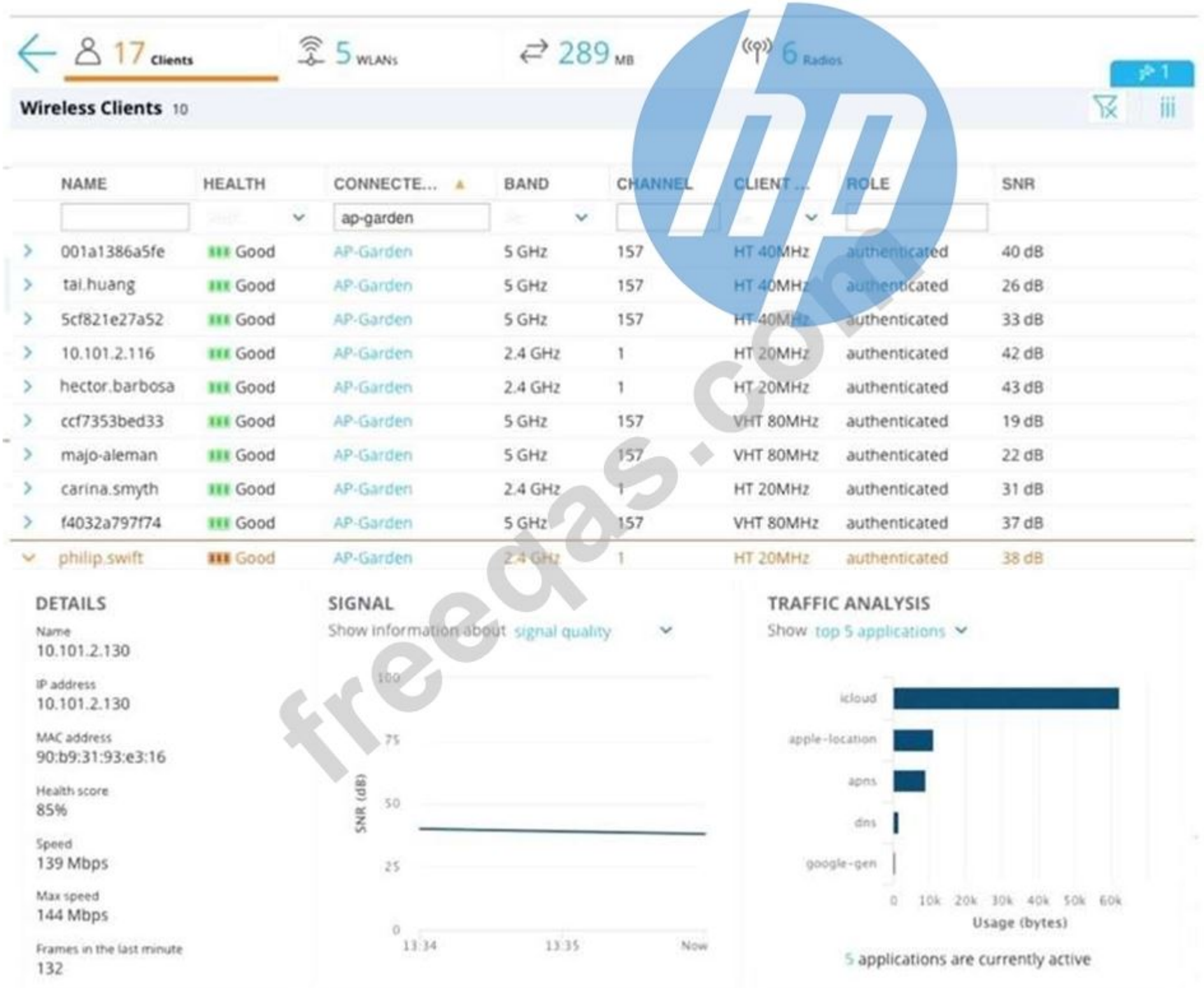
RADIO 2.4 GHZ - CHANNEL 1

Show information about channel utilization

RADIO 5 GHZ - CHANNEL 157E

Show information about channel utilization





A user reports slow connectivity to a network administrator when connecting to AP-Garden and suggests that there might be a problem with the WLAN. The user's device supports 802.11n in the 2.4 GHz band. The network administrator finds the user in the Mobility Master (MM) and reviews the output shown in the exhibit.

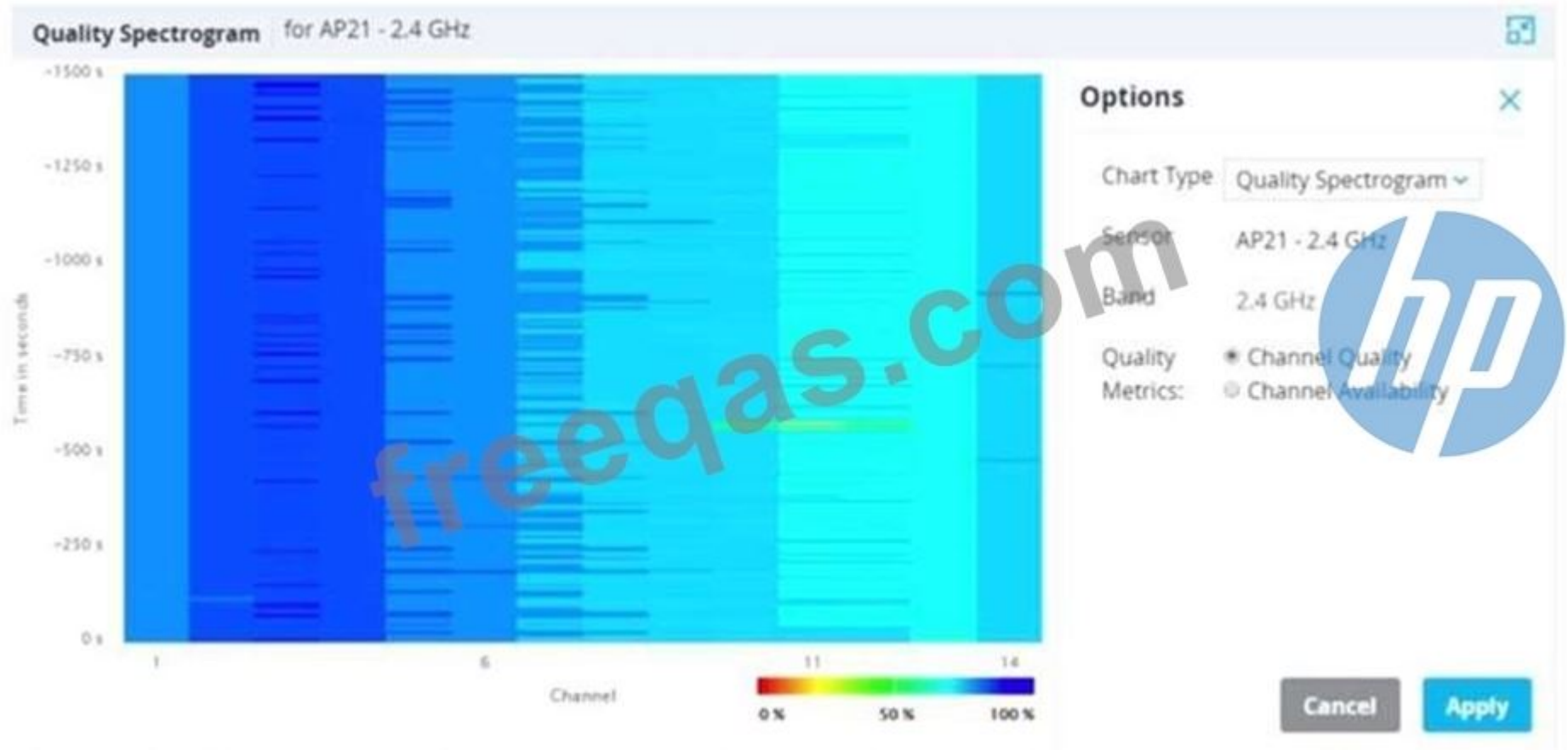
What can the network administrator conclude after analyzing the data?

A. 2.4Ghz band is currently congested, therefore a NIC upgrade to 802.11ac or higher is recommended so the user can move to 5Ghz.

B. User's SNR value over time is lower than recommended, therefore he should either get closer to the Access Point or increase the transmit power.

C. Channel usage is high and though this device has high speed the overall client rate is low on AP-Garden. there could be a few clients monopolizing the airtime on both bands at low speeds.
D. 365s are low cost outdoor APs recommended for coverage design only. AP-Garden currently has more clients than recommended and is getting congested.
Answer: (SHOW ANSWER)

NEW QUESTION: 7
Refer to the exhibit.



Based on the output shown in the exhibit, which channel offers the highest quality?
A. Channel 6
B. Channel 1
C. Channel 11
D. Channel 14
Answer: A (LEAVE A REPLY)

NEW QUESTION: 8
A network administrator wants to permit explicit SSH, FTP and HHTP(s) access to servers in the 10.100.20.5 to 10.100.20.31 range, all devices in 10.100.21.0/24 network, and a host with IP address 10.100.22.70. The services must work properly at all times.
Which configuration scripts accomplish this task with the fewer number of lines, while avoiding access to other devices not included in these ranges? (Choose two.)

A.

```
ip access-list session access2servers
    user alias file&web_servers svc-http permit
    user alias file&web_servers svc-https permit
    user alias file&web_servers svc-ssh permit
    user alias file&web_servers svc-ftp permit
```

B.

```
netdestination file&web_servers
    host 10.100.22.70
    range 10.100.20.5 to 10.100.20.21
    range 10.100.20.22 to 10.100.20.31
    network 10.100.21.0 255.255.255.0
```

C.

```
netdestination file&web_servers
host 10.100.22.70
network 10.100.20.0 255.255.255.0
network 10.100.21.0 255.255.255.0
```

D.

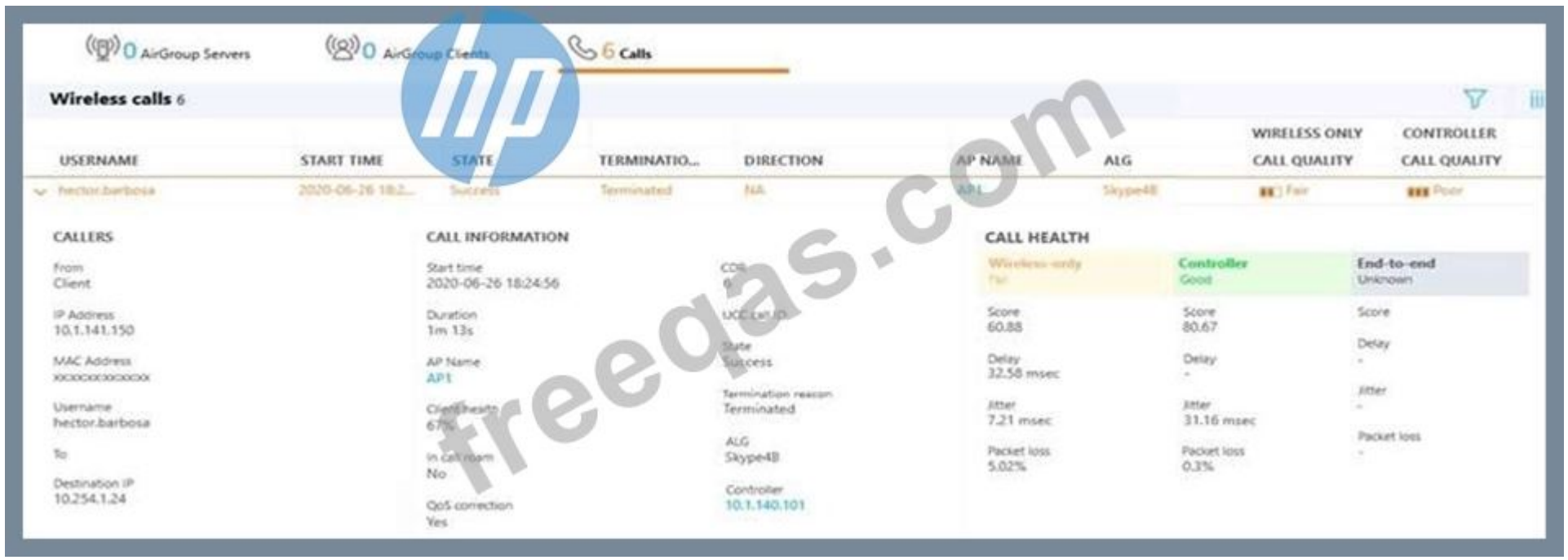
```
netdestination file&web_servers
    host 10.100.22.70
    network 10.100.20.0 255.255.255.0
    network 10.100.21.0 255.255.255.0
```

E.

```
ip access-list session access2servers
    user alias file&web_servers tcp 20 permit
    user alias file&web_servers tcp 21 permit
    user alias file&web_servers tcp 22 permit
    user alias file&web_servers tcp 80 permit
    user alias file&web_servers tcp 443 permit
```

A. Option D
B. Option E
C. Option B
D. Option C
E. Option A
Answer: (SHOW ANSWER)

NEW QUESTION: 9
Refer to the exhibit.



A network administrator has recently enabled WMM on the VAP's SSID profile and enabled UCC Skype4B ALG at the Mobility Master level. During testing, some voice and video conference calls were made, and it was concluded that the call quality has dramatically improved. However, end to end information isn't displayed in the call's details. Also, Skype4B app-sharing's performance is poor at times.
What must the administrator do next in order to enable end to end call visibility and QoS correction to app-sharing service?

A. Enable UCC monitoring on the "default-controller' mgmt.-server profile.

B. Increase the app-sharing DSCP value in the Skype4B ALG profile.

C. Enable the App-sharing ALG profile at both MM and MD hierarchy levels.

D. Deploy the SDN API Software in the Skype4B Solution and point to the MM.

Answer: (SHOW ANSWER)

NEW QUESTION: 10

Refer to the exhibit.

```
(MC1) [MDC] #show ip access-list no-webapps

ip access-list session no-webapps
no-webapps
----------
Priority  Source  Destination  Service  Application  Action                  TimeRange  Log  Expired  Queue  TOS  8021P  Blacklist  Mirror  DisScan  IPv4/6  Contract
--------  ------  -----------  -------  -----------  ------                  ---------  ---  -------  -----  ---  -----  ---------  ------  -------  ------  --------
1         user    any                   app facebook  deny send-deny-response                        Low                                          4
2         user    any                   app youtube   deny send-deny-response                        Low                                          4
3         user    any                   app netflix   deny send-deny-response                        Low                                          4
```

A network administrator completes the initial configuration dialog of the Mobility Controllers (MCs) and they join the Mobility Master (MM) for the first time. After the MM-MC association process, network administrator only creates AP groups, VAPs, and roles. Next, the network administrator proceeds with the configuration of the policies and creates the policy shown in the exhibit.
Which additional steps must be done to make sure this configuration takes effect over the contractor users?

A. Apply the policy in the contractors user role.
Enable deep packet inspection.
Reload the MCs.

B. Enable firewall visibility.
Enable web-content classification.
Reload the MCs.

C. Apply the policy in the contractors user role.
Enable deep packet inspection.

D. Enable firewall visibility.
Enable web-content classification.
Reload the MMs.

A. Option A

B. Option C

C. Option D

D. Option B

Answer: B (LEAVE A REPLY)

NEW QUESTION: 11

An organization wants to deploy a WLAN infrastructure that provides connectivity to these client categories:

* Employees
* Contractors
* Guest users
* Corporate IoT legacy devices that support no authentication or encryption Employees and contractors must authenticate with company credentials and get network access based on AD group membership. Guest users are required to authenticate with captive portal using predefined credentials. Only employees will run L2 encryption.

Which implementation plan fulfills the requirements while maximizing the channel usage?

A. Create VAP1 to run WPA2-AES and 802.1x authentication. VAP2 to run opensystem encryption with MAC authentication, and VAP3 to run opensystem with captive portal.

B. Create VAP1 to run WPA2-AES and 802.1x authentication. VAP2 to run opensystem encryption with MAC authentication, and VAP3 to run opensystem with captive portal and L2 fail through.

C. Create a single VAPto run WPA2-AES and 802.1x authentication. MAC authentication L2 fail through, captive portal, and VIA support.

D. Create VAP1 to run WPA2-AES and 802.1x authentication, and VAP2 to run opensystem encryption with MAC authentication and captive portal.

Answer: D (LEAVE A REPLY)

NEW QUESTION: 12

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.

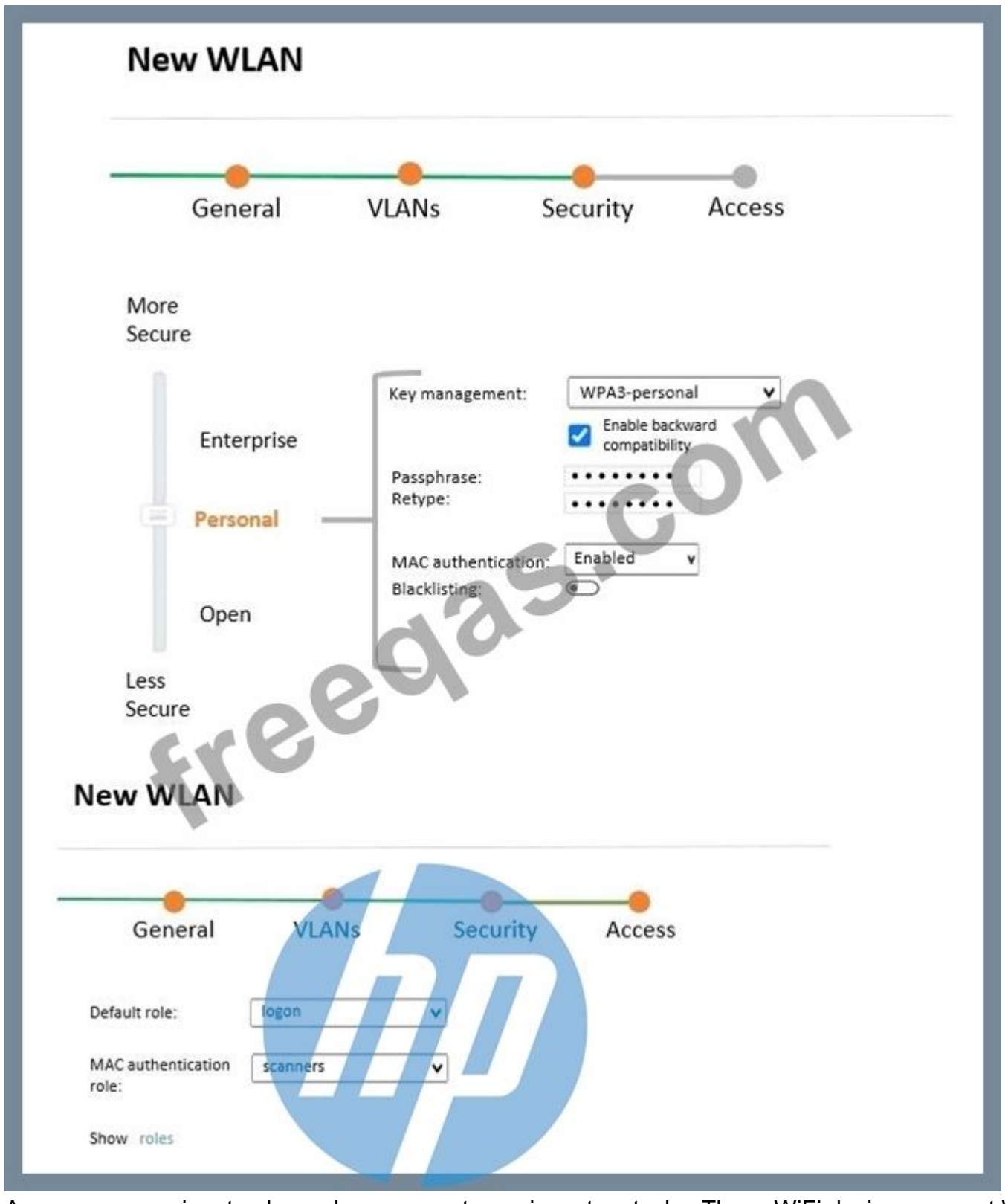
Since not all locations own public IP addresses, the security team is not able to configure strict firewall polices at the datacenter without disrupting some MM to Mobility Controller (MC) communications. They are also concerned about exposing the MMs to unauthorized inbound connection attempts.

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

A. Block all ports to the MMs except UDP 500 and 4500.
B. Block all inbound connections, and instruct the MM to initiate the connection to the MCs.
C. Install a PEFV license, and configure firewall policies that protect the MM.
D. Deploy an MC at the datacenter as a VPN concentrator.
Answer: (SHOW ANSWER)

NEW QUESTION: 13
An Aruba Mobility Master (MM) - Mobility Controller (MC) solution is connected to a wired network that is ready to prioritize DSCP marked traffic. A group of WMM-enabled clients sends traffic marked at L2 only.
What must the network administrator do to map those markings to DSCP equivalent values when traffic is received by the APs?
A. Enable traffic to be marked with session ACLs.
B. Enable WMM in the VAP profile.
C. Enable WMM in the SSID profile.
D. Enable Skype4Business ALG Support.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 14
Refer to the exhibit:



A company acquires ten barcode scanners to run inventory tasks. These WiFi devices support WPA2-PSK security only. The network administrator deploys a WLAN named scanners using the configuration shown in the exhibit.

What must the network administrator do next to ensure that the scanner devices successfully connect to their SSID?

A. Enable L2 Authentication Fail Through.

B. Set internal as the MAC authentication server group.

C. Add scanner MAC addresses in user derivation rules.

D. Add scanner MAC addresses in the internal database.

Answer: D (LEAVE A REPLY)

NEW QUESTION: 15
A company with 535 users deploys an Aruba solution with more than 1000 Aruba APs, two 7220 Mobility Controllers, and a single Mobility Master (MM) virtual appliance at the campus server farm. The MCs run a HA Fast failover group in dual mode and operate at 50% AP capacity.
If there is an MM or MC failure, the network administrator must ensure that the network is fully manageable and the MC load does not exceed 80%.
What can the network administrator do to meet these requirements?
A. Enable oversubscription in the HA group.
B. Create a cluster with AP load balancing.
C. Add an MM and enable DC redundancy.
D. Place the APs in two different AP-Groups.
E. Place the APs in the same hierarchy level.
F. Add an MC and an MM in the server farm.
Answer: (SHOW ANSWER)

NEW QUESTION: 16
Refer to the exhibit.

```
(MC1) [mynode] #show ap database

AP Database
-----------
Name  Group              AP Type  IP Address    Status           Flags  Switch IP     Standby IP
----  -----              -------  ----------    ------           -----  ----------    ----------
AP1   Main-Campus-SC-B1  355      10.1.145.150  Up 1d:7h:21m:41s 2      10.1.140.100  0.0.0.0
AP2   Main-Campus-SC-B1  355      10.1.146.150  Up 1d:7h:21m:46s 2      10.1.140.100  0.0.0.0

Flags: 1 = 802.1x authenticated AP use EAP-PEAP; 1+ = 802.1x use EST; 1- = 802.1x use factory cert; 2 = Using IKE version 2
       B = Built-in AP; C = Cellular RAP; D = Dirty or no config
       E = Regulatory Domain Mismatch; F = AP failed 802.1x authentication
       G = no such group; I = Inactive; J = USB cert at AP; L = Unlicensed
       M = Mesh node
       N = Duplicate name; P = PPPoe AP; R = Remote AP; R- = Remote AP requires Auth;
       S = Standby-mode AP; U = Unprovisioned; X = Maintenance Mode
       Y = Mesh Recovery
       c = CERT-based RAP; e = Custom EST cert; f = No Spectrum FFT support
       i = Indoor; o = Outdoor; s = LACP striping; u = Custom-Cert RAP; z = Datazone AP

Total APs:2
(MC1) [MDC] #
(MC1) [MDC] #show lc-cluster group-membership

Cluster Enabled, Profile Name = "Cluster1"
Redundancy Mode On
Active Client Rebalance Threshold = 50%
Standby Client Rebalance Threshold = 75%
Unbalance Threshold = 5%
AP Load Balancing: Disabled
Cluster Info Table
------------------
Type IPv4 Address     Priority  Connection-Type  STATUS
---- ---------------  --------  ---------------  ------
self    10.1.140.100        10              N/A  ISOLATED (Leader)
```

After deploying several cluster pairs, the network administrator notices that all APs assigned to Cluster1 communicate with MC1 instead of being distributed between members of the cluster. Also, no IP addresses are shown under the Standby IP column.
What should the network administrator do to fix this situation?

A. Enable Cluster AP load balancing.
B. Apply the same cluster profile to both members.
C. Rename the cluster profile as "CLUSTER1".
D. Place MCs at the same hierarchical group level.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 17
Refer to the exhibit.

```
(MC2)  [MDC] #show user mac xx:xx:xx:xx:xx:xx
This operation can take a while depending on number of users. Please be patient ....


Name: contractor14, IP:10.1.141.150, MAC: xx:xx:xx:xx:xx:xx, Age: 00:00:00
Role: contractor (how: ROLE_DERIVATION_DOT1X_VSA), ACL: 128/0
Authentication: Yes, status: successful, method: 802.1x, protocol: EAP-PEAP, server: ClearPass.23
Authentication Servers: dot1x authserver: ClearPass.23, mac authserver:
Bandwidth = No Limit
Bandwidth = No Limit
Role Derivation: ROLE_DERIVATION_DOT1X_VSA
```

A network administrator is evaluating a deployment to validate that a user is assigned the proper role and reviews the output in the exhibit.
How is the role assigned to user?
A. The MC assigned the role based on Aruba VSAs.
B. The MC assigned the machine authentication default user role.
C. The MC assigned the default role based on the authentication method.
D. The MC assigned the role based on server derivation rules.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 18
Refer to the exhibits.
Exhibit 1

```
(MC2) [MDC] #show user
This operation can take a while depending on number of users. Please be patient ....

Users
-----
    IP              MAC              Name    Role                    Age(d:h:m) Auth    VPN link  AP name  Roaming  Essid/Bssid/Phy
     Profile  Forward mode Type      Host Name  User Type
---------   ----------              -----   ----                    ---------- ----    -------  -------  -------  --------------
    -------     ------------        -----  --------  -------
192.168.14.101 xx:xx:xx:xx:xx:xx          guest-guest-logon       00:00:32                  AP1      Wireless  Guest/yy:yy:yy:yy:yy:yy/a-
VHT  Guest   tunnel        Win 10          WIRELESS

User Entries: 1/1
 Curr/Cum Alloc:2/5 Free:0/3 DVN:2 AllocErr:0 FreeErr:0
```

Exhibit 2

```
(MC2) [MDC] #show rights guest-guest-logon

Valid = 'Yes'
CleanedUp = 'No'
Derived Role = 'guest-guest-logon'
  Up BW:No Limit   Down BW:No Limit
  L2TP Pool = default-l2tp-pool
  PPTP Pool = default-pptp-pool
  Number of users referencing it = 2
  Periodic reauthentication: Disabled
  DPI Classification: Enabled
  Youtube education: Disabled
  Web Content Classification: Enabled
  IP-Classification Enforcement: Enabled
  ACL Number = 98/0
  Openflow: Enabled
  MaxSessions = 65535

  Check CP Profile for Accounting = TRUE
  Captive Portal profile = default
```

Exhibit 3

```
(MC2) [MDC] #show aaa authentication captive-portal Guest

Captive Portal Authentication Profile "Guest"
---------------------------------------------
Parameter                                   Value
---------                                   -----
Default Role                                guest
Default Guest Role                          guest
Server Group                                Guest
Redirect Pause                              10 sec
User Login                                  Enabled
Guest Login                                 Disabled
Logout popup window                         Enabled
Use HTTP for authentication                 Disabled
Logon wait minimum wait                     5 sec
Logon wait maximum wait                     10 sec
Logon wait CPU utilization threshold        60%
Max Authentication failures                 0
Show FQDN                                   Disabled
Authentication Protocol                     PAP
Login page                                  https://cp.mycompany.com/guest/web_login.php
Welcome page                                /auth/welcome.html
Show Welcome Page                           Yes
```


Exhibit 4

```
(MC2) [MDC] #show aaa authentication captive-portal default

Captive Portal Authentication Profile "default"
-----------------------------------------------
Parameter                                   Value
---------                                   -----
Default Role                                guest
Default Guest Role                          guest
Server Group                                Guest
Redirect Pause                              10 sec
User Login                                  Enabled
Guest Login                                 Disabled
Logout popup window                         Enabled
Use HTTP for authentication                 Disabled
Logon wait minimum wait                     5 sec
Logon wait maximum wait                     10 sec
Logon wait CPU utilization threshold        60%
Max Authentication failures                 0
Show FQDN                                   Disabled
Authentication Protocol                     PAP
Login page                                  /auth/index.html
Welcome page                                /auth/welcome.html
Show Welcome Page                           Yes
Add switch IP addresses in the redirection URL  Disabled
```

```
(MC2) [MDC] #show aaa server-group default

Fail Through: No
Load Balance: No

Auth Servers
------------
Name        Server-Type    trim-FQDN   Match-Type  Match-Op  Match-Str
----        -----------    ---------   ----------  --------  ---------
Internal    Internal       No

Role/VLAN derivation rules
--------------------------
Priority   Attribute   Operation   Operand   Type    Action    Value   Validated
--------   ---------   ---------   -------   ----    ------    -----   ---------
1          role        value-of              String  set role          No
```

A captive portal-based solution is deployed in a Mobility Master (MM) - Mobility Controller (MC) network. A wireless station connects to the network and attempts the authentication process. The outputs are shown in the exhibits.

Which names correlate with the authentication and captive portal servers?

A. ClearPass.23 is the authentication server, and MC2 is the captive portal server.

B. Internal database in MC2 is the authentication server, and cp.mycompany.com is the captive portal server.
C. ClearPass.23 is the authentication server, and cp.mycompany.com is the captive portal server.
D. cp.mycompany.com is the authentication server, and ClearPass.23 is the captive portal server.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 19
A company plans to build a resort that includes a hotel with 1610 rooms, a casino, and a convention center. The company is interested in a mobility solution that provides scalability and a service-based approach, where they can rent the WLAN infrastructure at the convention center to any customer (tenant) that hosts events at the resort.
The solution should provide:
* Seamless roaming when users move from the hotel to the casino or the convention center
* Simultaneous propagation of the resort and customer-owned SSIDs at the convention center
* Null management access upon resort network infrastructure to the customers (tenants)
* Configuration and monitor rights of rented SSIDs to the customers (tenants) Which deployment meets the requirements?
A. Deploy IAPs with zone based SSIDs and manage them with different central accounts.
B. Deploy an MM-MC infrastructure with multizone AP's, with one zone for tenant SSIDs.
C. Deploy an MM-MC infrastructure, and create different hierarchy groups for MCs and APs
D. Deploy IAPs along with AirWave. and deploy role-based management access control.
E. Deploy IAPs. and manage them with different central accounts.
Answer: E (LEAVE A REPLY)