Free Questions for HPE7-A07 by actualtestdumps

Shared by Benjamin on 24-05-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: DragDrop

Match each Group Based Policy (GBP) rote description to its respective role ID.

Question 2

Question Type: MultipleChoice

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
```

Which wireless connection phase has Just been completed?

Options:

A- MAC Authentication and 4-way handshake

B- L3 authentication and encryption

C- 802.11 enhanced open association

D- L2 authentication and encryption

Answer:

D

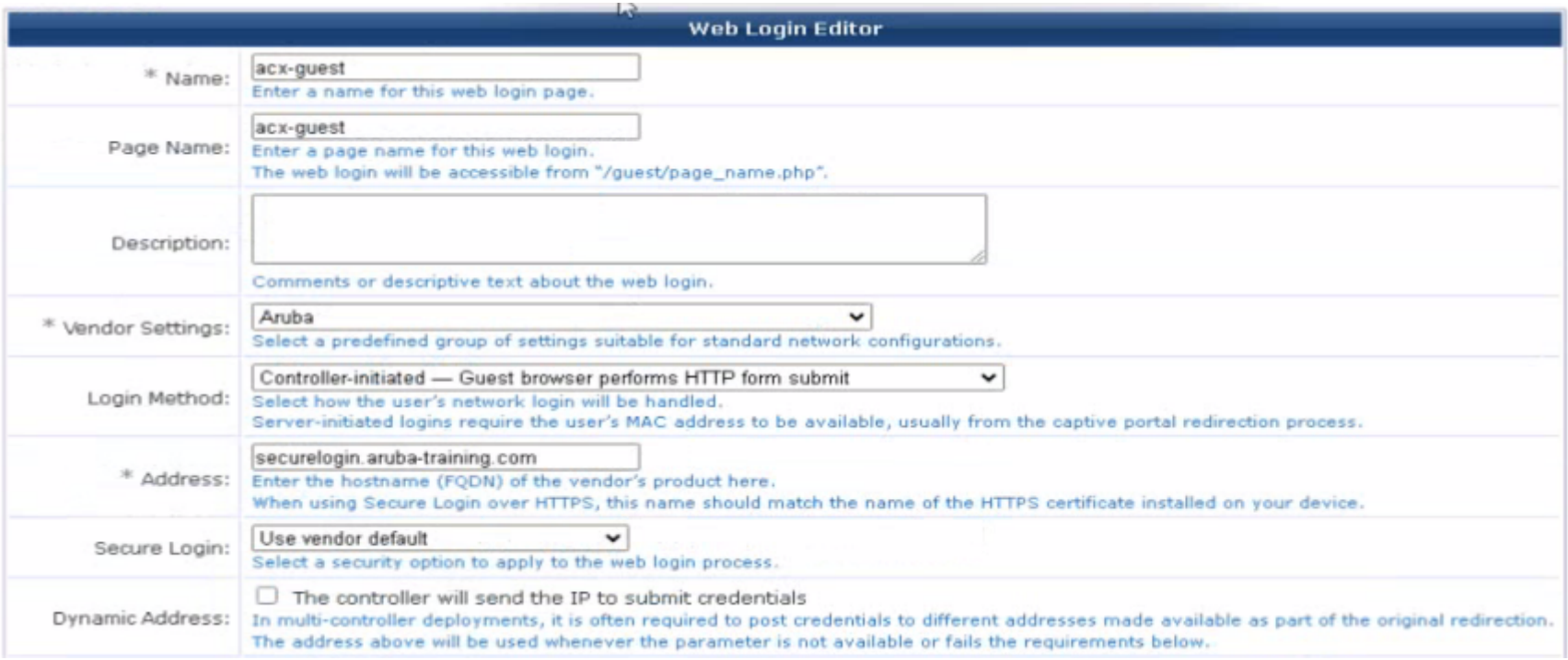
Explanation:

The wireless connection phase that has just been completed is L2 authentication and encryption. This phase includes processes such as the Extensible Authentication Protocol (EAP) exchange, RADIUS requests and responses, and the 4-way handshake which is characteristic of WPA2-AES encryption.

Question 3

Question Type: MultipleChoice

Exhibit.



Which would explain this issue?

Options:

A- HTTPS wildcard certificates are not supported

B- HTTPS certificate is not required in ClearPass Guest.

C- captiveportal-login aruba-training com needs to be entered m the Address field for the ClearPass Guest

D- '.aruba-training com needs to be entered in the Address field for the ClearPass Guest

Answer:

D

Explanation:

The correct address for the ClearPass Guest should match the FQDN of the HTTPS certificate installed on the device, which is often the FQDN of the vendor's product. This ensures secure and proper redirection to the captive portal during the authentication process. The FQDN should be entered in the Address field for ClearPass Guest configuration.

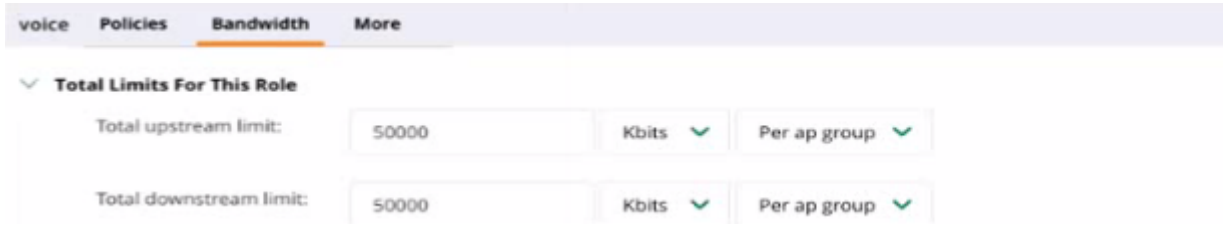
Question 4

Question Type: **MultipleChoice**

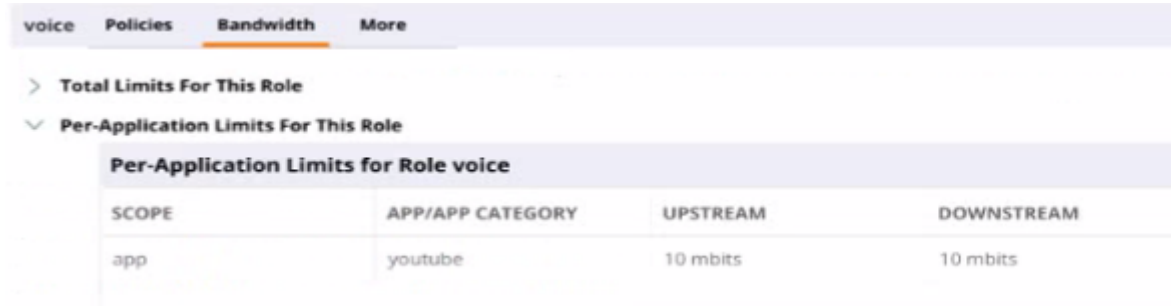
A network administrator accesses HPE Aruba Networking Central and notices that visitors consume too much internet bandwidth starving employee traffic when accessing an external service. Therefore, the administrator wants to limit wireless bandwidth to 60 Mops in both directions among all users in the voice rote and no more than 10 Mops in both directions for YouTube traffic. Deep packet inspection, web content classification, and firewall visibility are enabled.

Which configurations are required to accomplish this task? (Select two.)

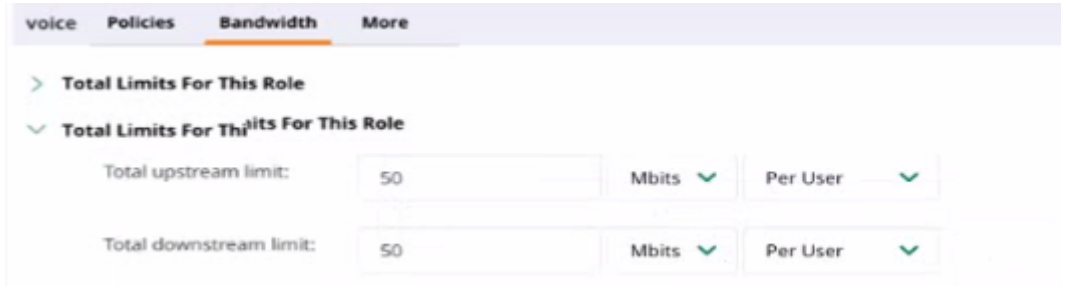
A)


voice
Policies
Bandwidth
More
Total Limits For This Role
Total upstream limit:
50000
Kbits
Per ap group
Total downstream limit:
50000
Kbits
Per ap group

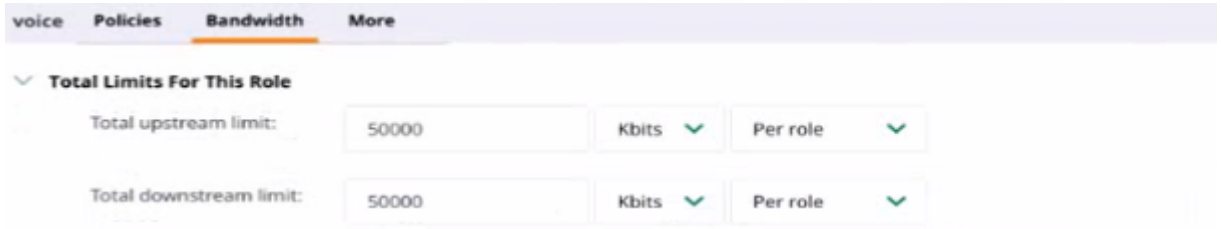
B)


voice
Policies
Bandwidth
More
Total Limits For This Role
Per-Application Limits For This Role
Per-Application Limits for Role voice
SCOPE
APP/APP CATEGORY
UPSTREAM
DOWNSTREAM
app
youtube
10 mbits
10 mbits

C)


voice
Policies
Bandwidth
More
Total Limits For This Role
Total Limits For Thi its For This Role
Total upstream limit:
50
Mbits
Per User
Total downstream limit:
50
Mbits
Per User

D)



Options:

A- Option A

B- Option B

C- Option C

D- Option D

Answer:

B, D

Explanation:

To achieve the bandwidth limits set by the network administrator, both per-application and total limits need to be configured. Option B shows the configuration for setting a per-application bandwidth limit, which can restrict YouTube traffic to 10 Mbps in both directions. Option D shows the configuration for setting a total bandwidth limit for all users within the voice role to 50000 Kbps (or 50 Mbps), satisfying the requirement to restrict total wireless bandwidth. By applying these configurations in HPE Aruba Networking Central, the

administrator will successfully implement the necessary controls to ensure that visitor traffic does not impede the network performance for employee traffic, aligning with the capabilities of Aruba solutions to manage and prioritize network resources effectively.

Question 5

Question Type: **MultipleChoice**

A customer is planning to add loT devices that connect wirelessly to the existing 802.1X SSlD. The customer will use ClearPass to authenticate the IoT devices by MAC address but other devices will still need to authenticate by only 802 1X

Exhibit.

```
wlan ssid-profile Employee
 enable
 index 0
 type employee
 essid Employee
 utf8
 opmode wpa3-aes-gcm-256
 max-authentication-failures 2
 vlan 100
 auth-server CPPM1
 rf-band all
 captive-portal disable
 mac-authentication
 dtim-period 1
 broadcast-filter none
 radius-accounting
 radius-interim-accounting-interval 10
```

The customer provided the current configuration and reported their non-loT 802. IX devices are no longer able to connect. Which configuration change can be made to fix the issue?

Options:

A- Modify opmode wpa3-aes-gcm-256 to opmode wpa2-aes

B- Add i2-autn-fairtnrougn to the WLAN configuration

C- Remove mac-authentication from the WLAN configuration

D- Modify max-authentication failures to 0.

Answer:

C

Explanation:

The existing configuration for the WLAN ssid-profile has enabled MAC authentication which, while suitable for IoT devices that may not support 802.1X, can interfere with the normal 802.1X authentication process for other devices. By removing the mac-authentication directive from the WLAN configuration, the non-IoT 802.1X devices should be able to connect without issues as the authentication process will not be disrupted by MAC authentication checks. This adjustment ensures that the WLAN ssid-profile is correctly aligned with the authentication requirements for both IoT and non-IoT devices within the network environment, conforming to the best practices for mixed-device WLAN configurations.

Question 6

Question Type: **MultipleChoice**

You want to configure an MTU of 9198 for a routed lag interface on a CX 6300 switch. Which configuration achieves this?

A)

```
interface lag 11 multi-chassis
    no shutdown
    ip mtu 9198
    ip address 10.1.1.1/24
    lacp mode active
    exit
!
interface 1/1/11
    mtu 9198
    lag 11
    exit
!
interface 1/1/12
    mtu 9198
    lag 11
    exit
```

B)

```
interface lag 11
    no shutdown
    ip address 10.1.1.1/24
    lacp mode active
    exit
!
interface 1/1/11
    mtu 9198
    lag 11
    exit
!
interface 1/1/12
    mtu 9198
    lag 11
    exit
```

C)

```
interface lag 11 multi-chassis
    lacp mode act
    exit
!
interface 1/1/11
    mtu 9198
    lag 11
    exit
!
interface 1/1/12
    mtu 9198
```

D)

```
interface lag 11
    no shutdown
    ip mtu 9198
    ip address 10.1.1.1/24
    lacp mode active
    exit
!
interface 1/1/11
    mtu 9198
    lag 11
    exit
!
interface 1/1/12
    mtu 9198
    lag 11
    exit
```

Options:

A- Option A

B- Option B

C- Option C

D- Option D

Answer:

A

Explanation:

In the context of ArubaOS-CX, particularly with the 6300 series switches, setting the MTU on a routed Link Aggregation Group (LAG) interface requires the interface lag id command in the configuration, specifying the LAG interface you're configuring. The ip mtu command is then used to set the desired MTU size for that LAG. Option A correctly shows this configuration process, where the MTU is set to 9198 for the LAG interface, in line with the requirements for routing larger frames, which could be necessary for certain applications or data flows that require jumbo frames.

The information related to the configuration of Aruba switches is consistent with the principles and guidelines found in the technical documentation for the ArubaOS-CX 6300 series switches, which emphasizes the importance of correct MTU settings for network performance and stability.