HPE6-A84$^{Q\&As}$

Aruba Certified Network Security Expert Written

Pass HP HPE6-A84 Exam with 100% Guarantee

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

https://www.geekcert.com/hpe6-a84.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

You are working with a developer to design a custom NAE script for a customer. You are helping the developer find the correct REST API resource to monitor.

Refer to the exhibit below.

What should you do before proceeding?

A. Go to the v1 API documentation interface instead of the v10.10 interface.

B. Use your Aruba passport account and collect a token to use when trying out API calls.

C. Enable the switch to listen to REST API calls on the default VRF.

D. Make sure that your browser is set up to store authentication tokens and cookies.

Correct Answer: B

The exhibit shows the ArubaOS-CX REST API documentation interface, which allows you to explore the available resources and try out the API calls using the "Try it out" button. However, before you can use this feature, you need to authenticate yourself with your Aruba passport account and collect a token that will be used for subsequent requests. This token will expire after a certain time, so you need to refresh it periodically. You can find more details about how to use the documentation interface and collect a token in the ArubaOS-CX REST API Guide1.

QUESTION 2

Refer to the scenario.

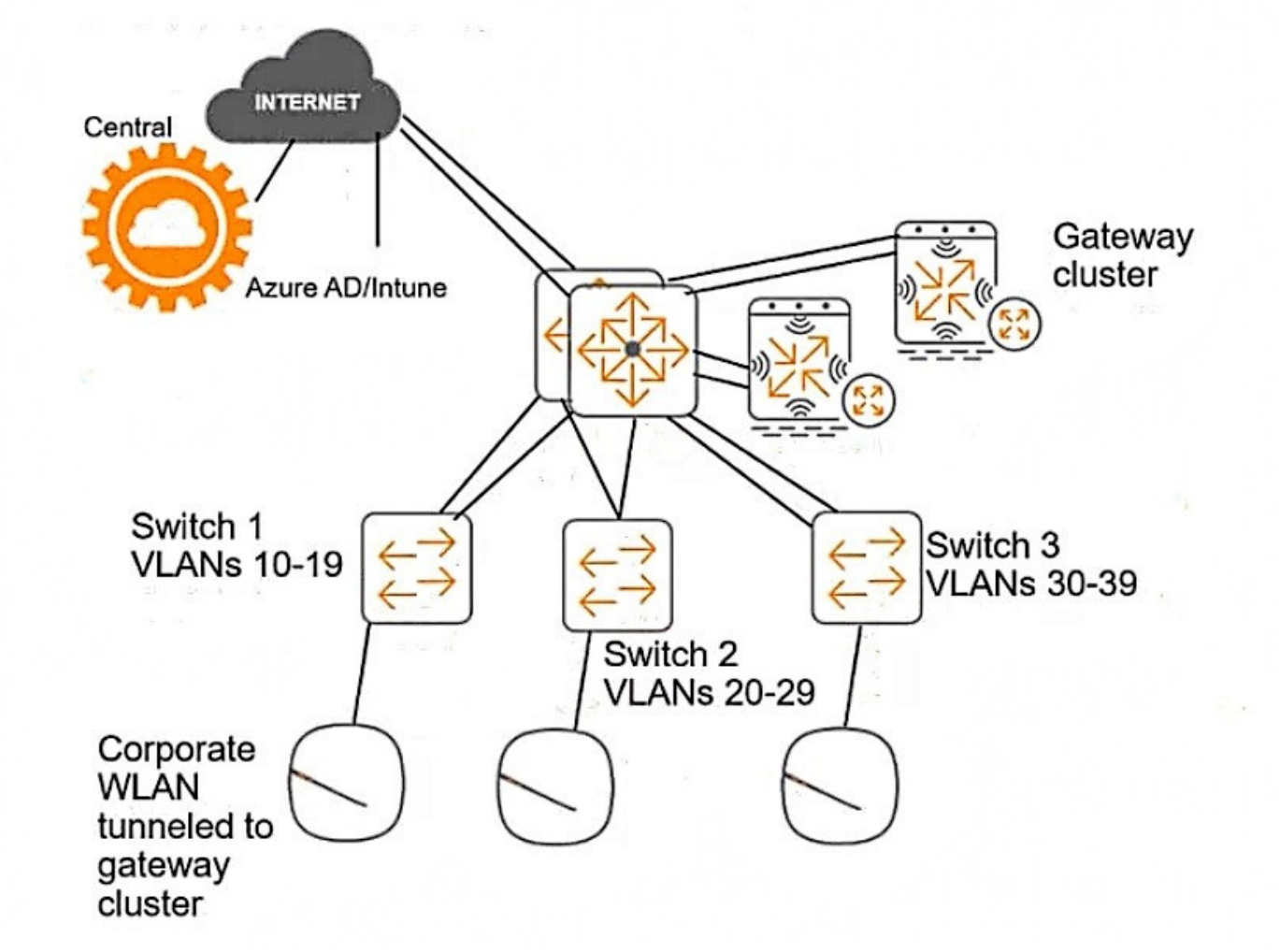
This customer is enforcing 802.1X on AOS-CX switches to Aruba ClearPass Policy Manager (CPPM). The customer wants switches to download role settings from CPPM. The "reception-domain" role must have these settings:

-- Assigns clients to VLAN 14 on switch 1, VLAN 24 on switch 2, and so on.

-- Filters client traffic as follows:

-- Clients are permitted full access to 10.1.5.0/24 and the Internet

-- Clients are denied access to 10.1.0.0/16 The switch topology is shown here:



How should you configure the VLAN setting for the reception role?

A. Assign a consistent name to VLAN 14, 24, or 34 on each access layer switch and reference that name in the enforcement profile VLAN settings.

B. Configure the enforcement profile as a downloadable role, but specify only the role name and leave the VLAN undefined. Then define a \\'reception\\' role with the correct VLAN setting on each individual access layer switch.

C. Assign a number-based ID to the access layer switches. Then use this variable in the enforcement profile VLAN settings: %(NAS-ID]4.

D. Create a separate enforcement profile with a different VLAN ID for each switch. Add all profiles to the profile list in the appropriate enforcement policy rule.

Correct Answer: A

According to the AOS-CX User Guide, one way to configure the VLAN setting for the reception role is to assign a consistent name to VLAN 14, 24, or 34 on each access layer switch and reference that name in the enforcement profile VLAN settings. This way, the switches can download the role settings from CPPM and apply the correct VLAN based on the name, rather than the ID. For example, the enforcement profile VLAN settings could be:

```
vlan-name reception-vlan
```

And the VLAN configuration on each switch could be:

```
vlan 14
name reception-vlan
exit
```

```
vlan 24
name reception-vlan
exit
```

```
vlan 34
name reception-vlan
exit
```

QUESTION 3

Refer to the scenario.

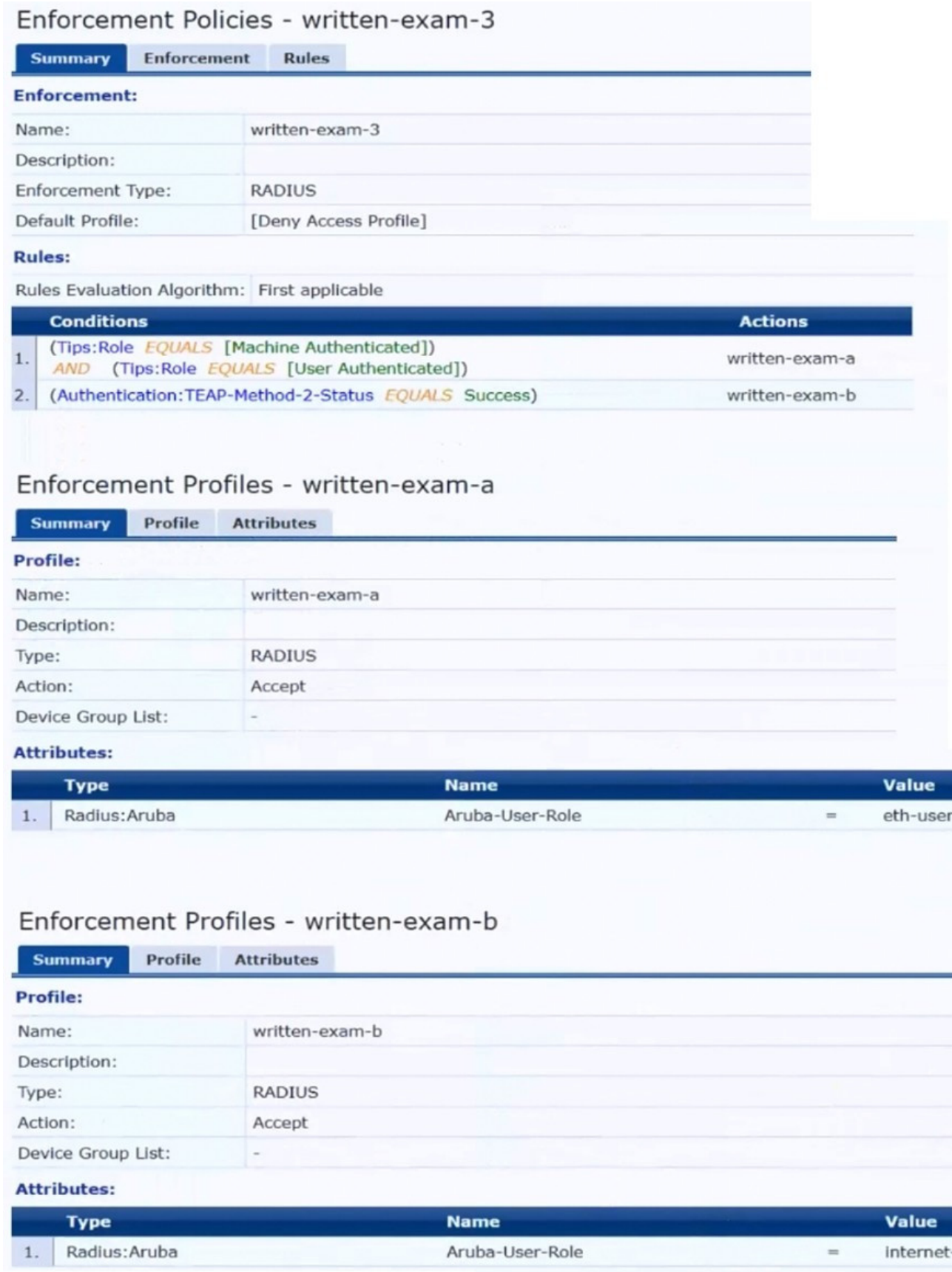
A customer has an Aruba ClearPass cluster. The customer has AOS-CX switches that implement 802.1X authentication to ClearPass Policy Manager (CPPM).

Switches are using local port-access policies.

The customer wants to start tunneling wired clients that pass user authentication only to an Aruba gateway cluster. The gateway cluster should assign these clients to the "eth- internet" role. The gateway should also handle assigning clients

to their VLAN, which is VLAN 20.

The plan for the enforcement policy and profiles is shown below:



Enforcement Policies - written-exam-3

Summary | Enforcement | Rules

Enforcement:

Name:	written-exam-3
Description:	
Enforcement Type:	RADIUS
Default Profile:	[Deny Access Profile]

Rules:

Rules Evaluation Algorithm: First applicable

	Conditions	Actions
1.	(Tips:Role EQUALS [Machine Authenticated]) AND (Tips:Role EQUALS [User Authenticated])	written-exam-a
2.	(Authentication:TEAP-Method-2-Status EQUALS Success)	written-exam-b

Enforcement Profiles - written-exam-a

Summary | Profile | Attributes

Profile:

Name:	written-exam-a
Description:	
Type:	RADIUS
Action:	Accept
Device Group List:	-

Attributes:

	Type	Name		Value
1.	Radius:Aruba	Aruba-User-Role	=	eth-user

Enforcement Profiles - written-exam-b

Summary | Profile | Attributes

Profile:

Name:	written-exam-b
Description:	
Type:	RADIUS
Action:	Accept
Device Group List:	-

Attributes:

	Type	Name		Value
1.	Radius:Aruba	Aruba-User-Role	=	internet-only

The gateway cluster has two gateways with these IP addresses:

Gateway 1

1.

VLAN 4085 (system IP) = 10.20.4.21

2.

VLAN 20 (users) = 10.20.20.1

3.

VLAN 4094 (WAN) = 198.51.100.14

Gateway 2

1.

VLAN 4085 (system IP) = 10.20.4.22

2.

VLAN 20 (users) = 10.20.20.2

3.

VLAN 4094 (WAN) = 198.51.100.12

VRRP on VLAN 20 = 10.20.20.254

The customer requires high availability for the tunnels between the switches and the gateway cluster. If one gateway falls, the other gateway should take over its tunnels. Also, the switch should be able to discover the gateway cluster regardless of whether one of the gateways is in the cluster.

Assume that you are using the "myzone" name for the UBT zone.

Which is a valid minimal configuration for the AOS-CX port-access roles?

A. port-access role eth-internet gateway-zone zone myzone gateway-role eth-user

B. port-access role internet-only gateway-zone zone myzone gateway-role eth-internet

C. port-access role eth-internet gateway-zone zone myzone gateway-role eth-internet vlan access 20

D. port-access role internet-only gateway-zone zone myzone gateway-role eth-internet vlan access 20

Correct Answer: B

The UBT solution requires that the edge ports on the switches are configured in VLAN trunk mode, not access mode. This is because the UBT solution uses a special VLAN (VLAN 4095 by default) to encapsulate the user traffic and tunnel it to the gateway. The edge ports need to allow this VLAN as well as any other VLANs that are used for management or control traffic. Therefore, the edge ports should be configured as VLAN trunk ports and allow the necessary VLANs

QUESTION 4

You are reviewing an endpoint entry in ClearPass Policy Manager (CPPM) Endpoints Repository.

What is a good sign that someone has been trying to gain unauthorized access to the network?

A. The entry shows multiple DHCP options under the fingerprints.

B. The entry shows an Unknown status.

C. The entry shows a profile conflict of having a new profile of Computer for a profiled Printer.

D. The entry lacks a hostname or includes a hostname with long seemingly random characters.

Correct Answer: C

A profile conflict occurs when ClearPass Policy Manager (CPPM) detects a change in the device category or OS family of an endpoint that has been previously profiled. This could indicate that someone has spoofed the MAC address of a legitimate device and is trying to gain unauthorized access to the network. For example, if an endpoint that was previously profiled as a Printer suddenly shows a new profile of Computer, this could be a sign of an attack. You can find more information about profile conflicts and how to resolve them in the ClearPass Policy Manager User Guide1. The other options are not necessarily signs of unauthorized access, as they could have other explanations. For example, multiple DHCP options under the fingerprints could indicate that the device has connected to different networks or subnets, an Unknown status could indicate that the device has not been authenticated yet, and a lack of hostname or a random hostname could indicate that the device has not been configured properly or has been reset to factory settings.

QUESTION 5

Refer to the scenario.

A customer requires these rights for clients in the "medical-mobile" AOS firewall role on Aruba Mobility Controllers (MCs):

1.

Permitted to receive IP addresses with DHCP

2.

Permitted access to DNS services from 10.8.9.7 and no other server

3.

Permitted access to all subnets in the 10.1.0.0/16 range except denied access to 10.1.12.0/22

4.

Denied access to other 10.0.0.0/8 subnets

5.

Permitted access to the Internet

6.

Denied access to the WLAN for a period of time if they send any SSH traffic

7.

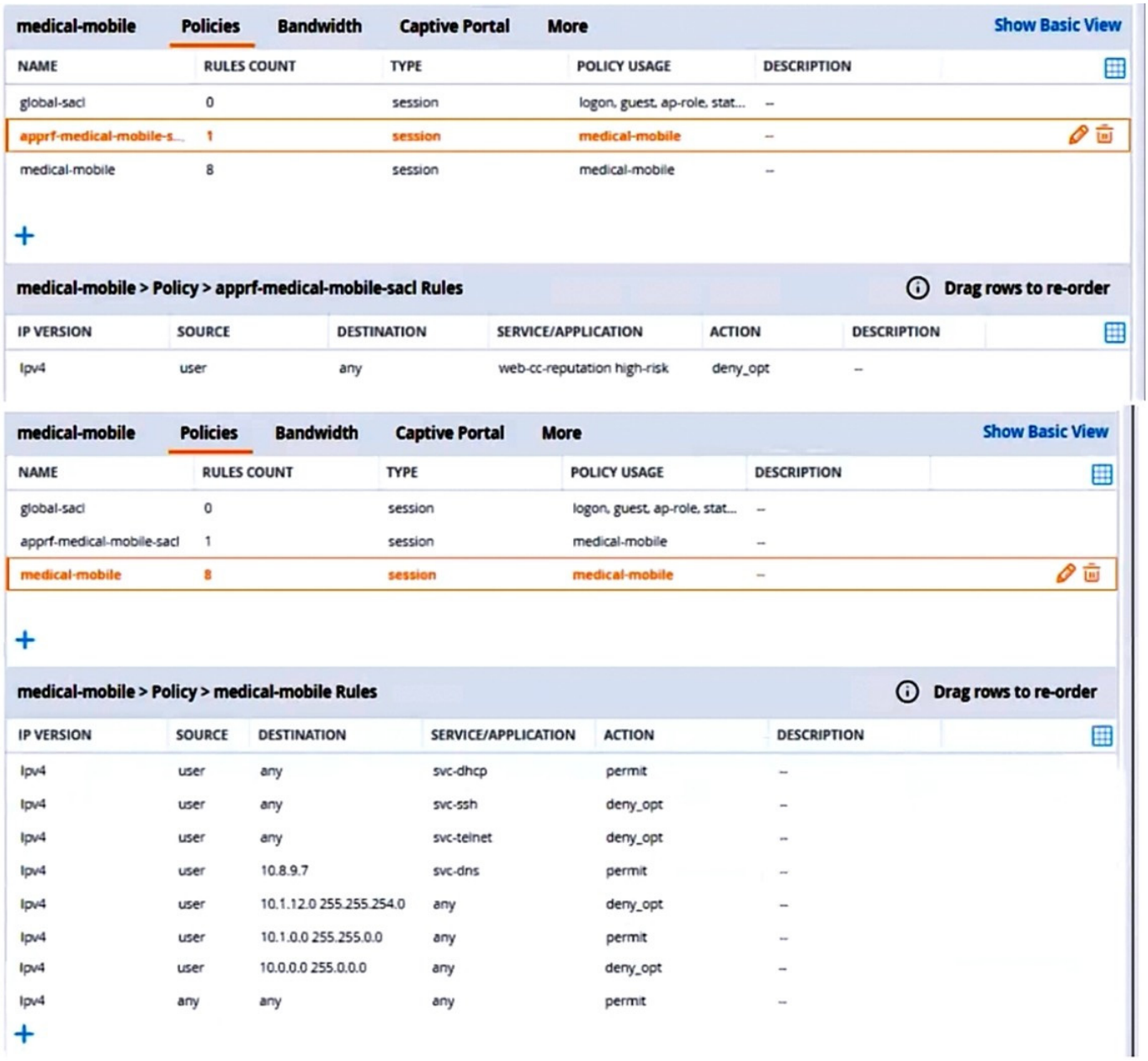
Denied access to the WLAN for a period of time if they send any Telnet traffic

8.

Denied access to all high-risk websites

External devices should not be permitted to initiate sessions with "medical-mobile" clients, only send return traffic.

The exhibits below show the configuration for the role.



medical-mobile | **Policies** | **Bandwidth** | **Captive Portal** | **More** | **Show Basic View**

NAME	RULES COUNT	TYPE	POLICY USAGE	DESCRIPTION
global-sacl	0	session	logon, guest, ap-role, stat...	--
apprf-medical-mobile-s...	1	session	medical-mobile	--
medical-mobile	8	session	medical-mobile	--

medical-mobile > Policy > apprf-medical-mobile-sacl Rules | Drag rows to re-order

IP VERSION	SOURCE	DESTINATION	SERVICE/APPLICATION	ACTION	DESCRIPTION
ipv4	user	any	web-cc-reputation high-risk	deny_opt	--

medical-mobile | **Policies** | **Bandwidth** | **Captive Portal** | **More** | **Show Basic View**

NAME	RULES COUNT	TYPE	POLICY USAGE	DESCRIPTION
global-sacl	0	session	logon, guest, ap-role, stat...	--
apprf-medical-mobile-sacl	1	session	medical-mobile	--
medical-mobile	8	session	medical-mobile	--

medical-mobile > Policy > medical-mobile Rules | Drag rows to re-order

IP VERSION	SOURCE	DESTINATION	SERVICE/APPLICATION	ACTION	DESCRIPTION
ipv4	user	any	svc-dhcp	permit	--
ipv4	user	any	svc-ssh	deny_opt	--
ipv4	user	any	svc-telnet	deny_opt	--
ipv4	user	10.8.9.7	svc-dns	permit	--
ipv4	user	10.1.12.0 255.255.254.0	any	deny_opt	--
ipv4	user	10.1.0.0 255.255.0.0	any	permit	--
ipv4	user	10.0.0.0 255.0.0.0	any	deny_opt	--
ipv4	any	any	any	permit	--

What setting not shown in the exhibit must you check to ensure that the requirements of the scenario are met?

A. That denylisting is enabled globally on the MCs\\' firewalls

B. That stateful handling of traffic is enabled globally on the MCs\\' firewalls and on the medical-mobile role.

C. That AppRF and WebCC are enabled globally and on the medical-mobile role

D. That the MCs are assigned RF Protect licenses

Correct Answer: C

AppRF and WebCC are features that allow the MCs to classify and control application traffic and web content based on predefined or custom categories 12. These features are required to meet the scenario requirements of denying access to

all high-risk websites and denying access to the WLAN for a period of time if they send any SSH or Telnet traffic.

To enable AppRF and WebCC, you need to check the following settings:

On the global level, you need to enable AppRF and WebCC under Configuration > Services > AppRF and Configuration > Services > WebCC, respectively 12. On the role level, you need to enable AppRF and WebCC under Configuration >

Security > Access Control > Roles > medical-mobile > AppRF and Configuration > Security > Access Control > Roles > medical-mobile > WebCC, respectively 12. You also need to make sure that the MCs have valid licenses for AppRF and

WebCC, which are included in the ArubaOS PEFNG license 3.