

# PASSTCERT

QUESTION & ANSWER

Higher Quality  
Better Service!

We offer free update service for one year  
[HTTP://WWW.PASSTCERT.COM](http://www.passtcert.com)

**Exam** : **HPE6-A84**

**Title** : Aruba Certified Network  
Security Expert Written  
Exam

**Version** : DEMO

1.You are designing an Aruba ClearPass Policy Manager (CPPM) solution for a customer. You learn that the customer has a Palo Alto firewall that filters traffic between clients in the campus and the data center. Which integration can you suggest?

- A. Sending Syslogs from the firewall to CPPM to signal CPPM to change the authentication status for misbehaving clients
- B. Importing clients' MAC addresses to configure known clients for MAC authentication more quickly
- C. Establishing a double layer of authentication at both the campus edge and the data center DMZ
- D. Importing the firewall's rules to program downloadable user roles for AOS-CX switches more quickly

**Answer: A**

2.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
<b>Enforcement:</b>		
Name:	written-exam-3	
Description:		
Enforcement Type:	RADIUS	
Default Profile:	[Deny Access Profile]	

<b>Rules:</b>		
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
<b>Profile:</b>		
Name:	written-exam-a	
Description:		
Type:	RADIUS	
Action:	Accept	
Device Group List:	-	

<b>Attributes:</b>			
Type	Name	Value	
1. Radius:Aruba	Aruba-User-Role	=	eth-user

## Enforcement Profiles - written-exam-b

Summary	Profile	Attributes
<b>Profile:</b>		
Name:	written-exam-b	
Description:		
Type:	RADIUS	
Action:	Accept	
Device Group List:	-	

<b>Attributes:</b>			
Type	Name	Value	
1. Radius:Aruba	Aruba-User-Role	=	internet-only

The gateway cluster has two gateways with these IP addresses:

- Gateway 1
  - o VLAN 4085 (system IP) = 10.20.4.21
  - o VLAN 20 (users) = 10.20.20.1
  - o VLAN 4094 (WAN) = 198.51.100.14
- Gateway 2
  - o VLAN 4085 (system IP) = 10.20.4.22
  - o VLAN 20 (users) = 10.20.20.2
  - o 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.

You are setting up the UBT zone on an AOS-CX switch.

Which IP addresses should you define in the zone?

- A. Primary controller = 10.20.4.21; backup controller = 10.20.4.22
- B. Primary controller = 198.51.100.14; backup controller = 10.20.4.21
- C. Primary controller = 10.20.4.21; backup controller, not defined
- D. Primary controller = 10.20.20.254; backup controller, not defined

**Answer: A**

3.Refer to the scenario.

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

Permitted to receive IP addresses with DHCP

Permitted access to DNS services from 10.8.9.7 and no other server

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

Denied access to other 10.0.0.0/8 subnets

Permitted access to the Internet

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

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

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					Polices	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					Polices	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	any	any	svc-dhcp	permit	--	
ipv4	user	10.8.9.7	svc-dns	permit	--	
ipv4	user	10.1.12.0 255.255.252.0	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	user	any	svc-telnet	deny_opt	--	
ipv4	user	any	svc-ssh	deny_opt	--	
ipv4	any	any	any	permit	--	

There are multiple issues with this configuration.

What is one change you must make to meet the scenario requirements? (In the options, rules in a policy are referenced from top to bottom. For example, "medical-mobile" rule 1 is "ipv4 any any svc-dhcp permit," and rule 8 is "ipv4 any any any permit".)

- A. In the "medical-mobile" policy, move rules 2 and 3 between rules 7 and 8.
- B. In the "medical-mobile" policy, change the subnet mask in rule 3 to 255.255.248.0.
- C. Move the rule in the "apprf-medical-mobile-sacl" policy between rules 7 and 8 in the "medical-mobile" policy.
- D. In the "medical-mobile" policy, change the source in rule 8 to "user."

**Answer: B**

4.A company has an Aruba ClearPass server at 10.47.47.8, FQDN radius.acnsxtest.local. This exhibit shows ClearPass Policy Manager's (CPPM's) settings for an Aruba Mobility Controller (MC).

The MC is already configured with RADIUS authentication settings for CPPM, and RADIUS requests between the MC and CPPM are working. A network admin enters and commits this command to enable dynamic authorization on the MC: `aaa rfc-3576-server 10.47.47.8`

But when CPPM sends CoA requests to the MC, they are not working.

This exhibit shows the RFC 3576 server statistics on the MC:

**RADIUS RFC 3576 Statistics**

```

-----
Server          Disconnect Req  Disconnect Acc  Disconnect Rej  No Secret  No Sess ID  Bad Auth
Invalid Req    Pkts Dropped  Unknown service  CoA Req  CoA Acc  CoA Rej  No perm
-----
10.47.47.8     0              0                0          0          0          0
0              0              0                0          0          0          0
    
```

How could you fix this issue?

- A. Change the UDP port in the MCs' RFC 3576 server config to 3799.
- B. Enable RadSec on the MCs' RFC 3676 server config.
- C. Configure the MC to obtain the time from a valid NTP server.
- D. Make sure that CPPM is using an ArubaOS Wireless RADIUS CoA enforcement profile.

**Answer: A**

5.Refer to the scenario.

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

Permitted to receive IP addresses with DHCP

Permitted access to DNS services from 10.8.9.7 and no other server

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

Denied access to other 10.0.0.0/8 subnets

Permitted access to the Internet

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

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

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.

The image shows two screenshots of a network configuration interface. The top screenshot displays the 'Policies' tab for the 'medical-mobile' role. It shows a table with columns: NAME, RULES COUNT, TYPE, POLICY USAGE, and DESCRIPTION. The 'apprf-medical-mobile-s...' policy is highlighted, showing 1 rule, session type, and medical-mobile usage. Below this, the 'medical-mobile' policy is shown with 8 rules. A '+' sign indicates more rules. The bottom screenshot shows the 'Rules' tab for the 'apprf-medical-mobile-sacl' policy. It displays a table with columns: IP VERSION, SOURCE, DESTINATION, SERVICE/APPLICATION, ACTION, and DESCRIPTION. A single rule is shown for IPv4, source 'user', destination 'any', service 'web-cc-reputation high-risk', and action 'deny\_opt'. The second screenshot shows the 'Rules' tab for the 'medical-mobile' policy. It displays a table with columns: IP VERSION, SOURCE, DESTINATION, SERVICE/APPLICATION, ACTION, and DESCRIPTION. Multiple rules are listed, including deny rules for SSH and Telnet, and permit rules for DHCP, DNS, and general traffic.

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

**Answer: C**



