HP

HPE6-A84 Exam

Aruba Certified Network Security Expert Written Exam
Questions & Answers
Demo

Version: 6.0

Question: 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

Explanation:

This option allows CPPM to receive real-time information about the network activity and security posture of the clients from the firewall, and then apply appropriate enforcement actions based on the configured policies 12. For example, if a client is detected to be infected with malware or violating the network usage policy, CPPM can quarantine or disconnect the client from the network 2.

Question: 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

Enforcement:

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

Rules:

Rules Evaluation Algorithm:	First applicable

	Conditions
1.	(Tips:Role *EQUALS* [Machine Authenticated]) *AND* (Tips:Role *EQUALS* [User Authenticated])
2.	(Authentication:TEAP-Method-2-Status *EQUALS* Success)

Enforcement Profiles - written-exam-a

Summary | Profile | Attributes

Profile:

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

Attributes:

	Type	Name
1.	Radius:Aruba	Aruba-User-Role

Enforcement Profiles - written-exam-b

Summary | Profile | Attributes

Profile:

Name:	written-exam-b
Description:	

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

Explanation:

To configure user-based tunneling (UBT) on an AOS-CX switch, you need to specify the IP addresses of the mobility gateways that will receive the tunneled traffic from the switch 1. The primary controller is the preferred gateway for the switch to establish a tunnel, and the backup controller is the alternative gateway in case the primary controller fails or becomes unreachable 1. The IP addresses of the gateways should be their system IP addresses, which are used for inter-controller communication and cluster discovery 2.
In this scenario, the customer has a gateway cluster with two gateways, each with a system IP address on VLAN 4085. Therefore, the switch should use these system IP addresses as the primary and backup controllers for UBT. The IP addresses of the gateways on VLAN 20 and VLAN 4094 are not relevant for UBT, as they are used for user traffic and WAN connectivity, respectively 2. The VRRP IP address on VLAN 20 is also not applicable for UBT, as it is a virtual IP address that is not associated with any specific gateway 3.
Therefore, the best option is to use 10.20.4.21 as the primary controller and 10.20.4.22 as the backup controller for UBT on the switch. This will ensure high availability and cluster discovery for the tunneled traffic from the switch to the gateway cluster 12.

Question: 3

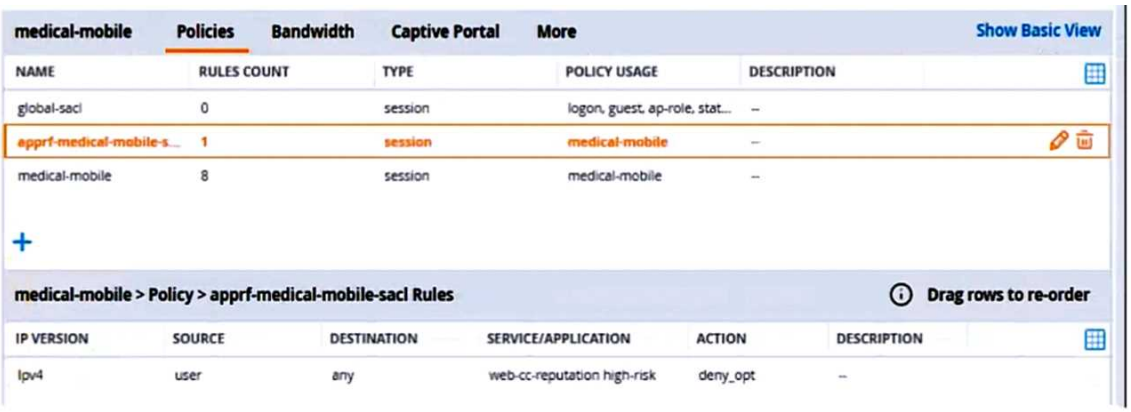
Refer to the scenario.

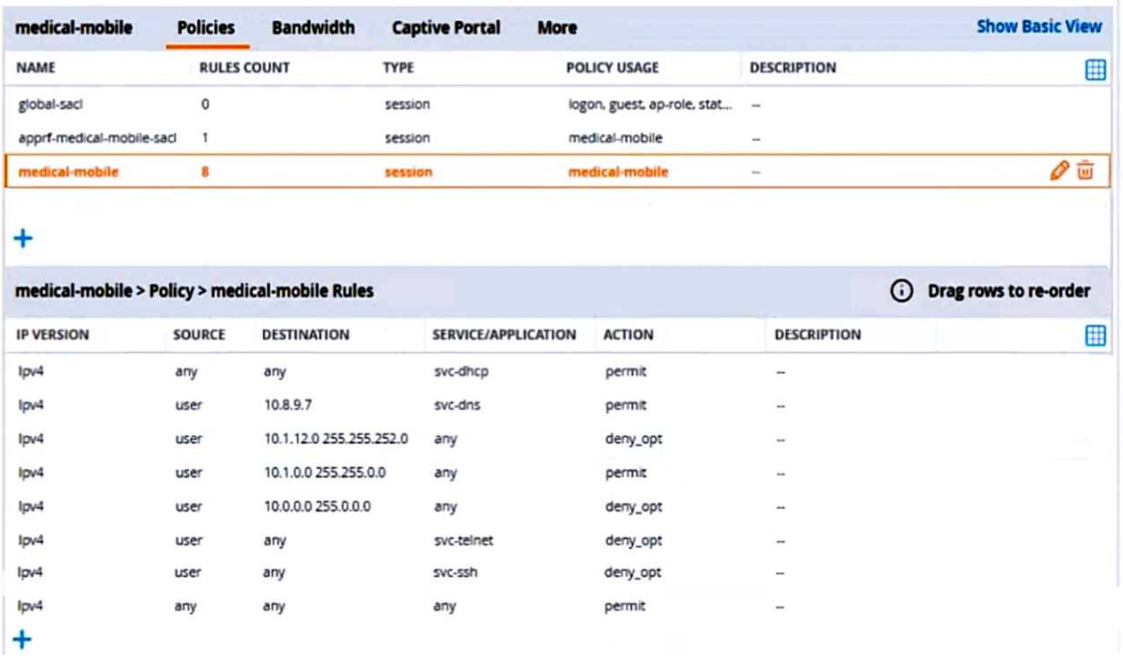
A customer requires these rights for clients in the “medical-mobile” AOS firewall role on Aruba Mobility Controllers (MCs):

- 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.





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.”

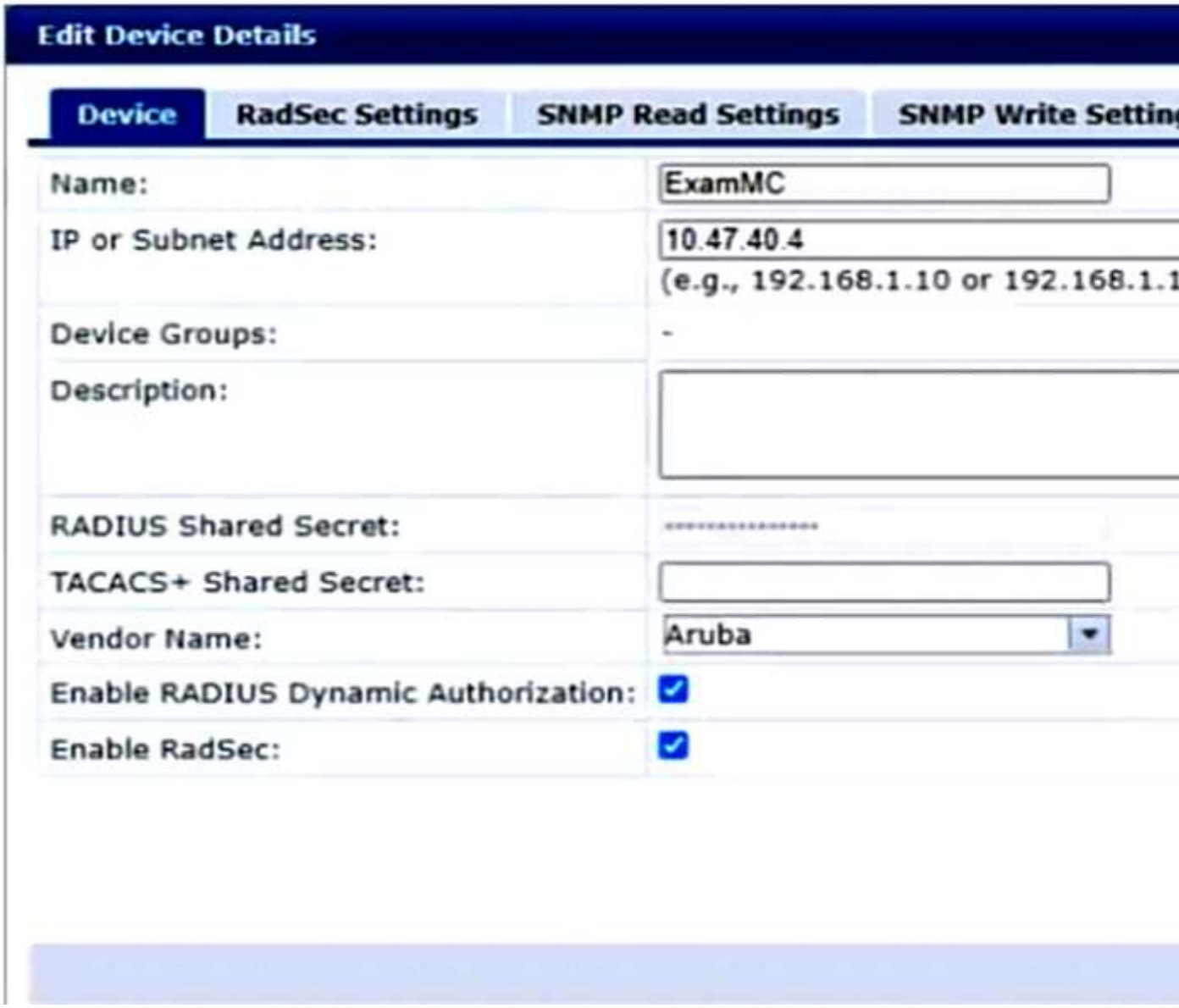
Answer: B

Explanation:

The subnet mask in rule 3 of the “medical-mobile” policy is currently 255.255.252.0, which means that the rule denies access to the 10.1.12.0/22 subnet as well as the adjacent 10.1.16.0/22 subnet 1. This is not consistent with the scenario requirements, which state that only the 10.1.12.0/22 subnet should be denied access, while the rest of the 10.1.0.0/16 range should be permitted access.
To fix this issue, the subnet mask in rule 3 should be changed to 255.255.248.0, which means that the rule only denies access to the 10.1.8.0/21 subnet, which includes the 10.1.12.0/22 subnet 1. This way, the rule matches the scenario requirements more precisely.

Question: 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

Explanation:

Dynamic authorization is a feature that allows CPPM to send change of authorization (CoA) or disconnect messages to the MC to modify or terminate a user session based on certain conditions or events 1. Dynamic authorization uses the RFC 3576 protocol, which is an extension of the RADIUS protocol 2.
To enable dynamic authorization on the MC, you need to configure the IP address and UDP port of the CPPM server as the RFC 3576 server on the MC 3. The default UDP port for RFC 3576 is 3799, but it can be changed on the CPPM server . The MC and CPPM must use the same UDP port for dynamic authorization to work properly 3.
In this scenario, the MC is configured with the IP address of the CPPM server (10.47.47.8) as the RFC 3576 server, but it is using the default UDP port of 3799. However, according to the exhibit, the CPPM server is using a different UDP port of 1700 for dynamic authorization . This mismatch causes the CoA requests from CPPM to fail on the MC, as shown by the statistics .
To fix this issue, you need to change the UDP port in the MCs' RFC 3576 server config to match the UDP port used by CPPM, which is 1700 in this case. Alternatively, you can change the UDP port in CPPM to match the default UDP port of 3799 on the MC. Either way, you need to ensure that both devices use the same UDP port for dynamic authorization 3 .

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):

- 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 | **Policies** | **Bandwidth** | **Captive Portal** | **More**

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

medical-mobile > Policy > apprf-medical-mobile-sacl Rules

IP VERSION	SOURCE	DESTINATION	SERVICE/APPLICATION
Ipv4	user	any	web-cc-reputation high-risk

medical-mobile | **Policies** | **Bandwidth** | **Captive Portal** | **More**

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

medical-mobile > Policy > medical-mobile Rules

IP VERSION	SOURCE	DESTINATION	SERVICE/APPLICATION	ACTION
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

Answer: C

Explanation:

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.