Vendor: HP

Exam Code: HPE6-A84

Exam Name: Aruba Certified Network Security Expert Written Exam

Version: DEMO

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

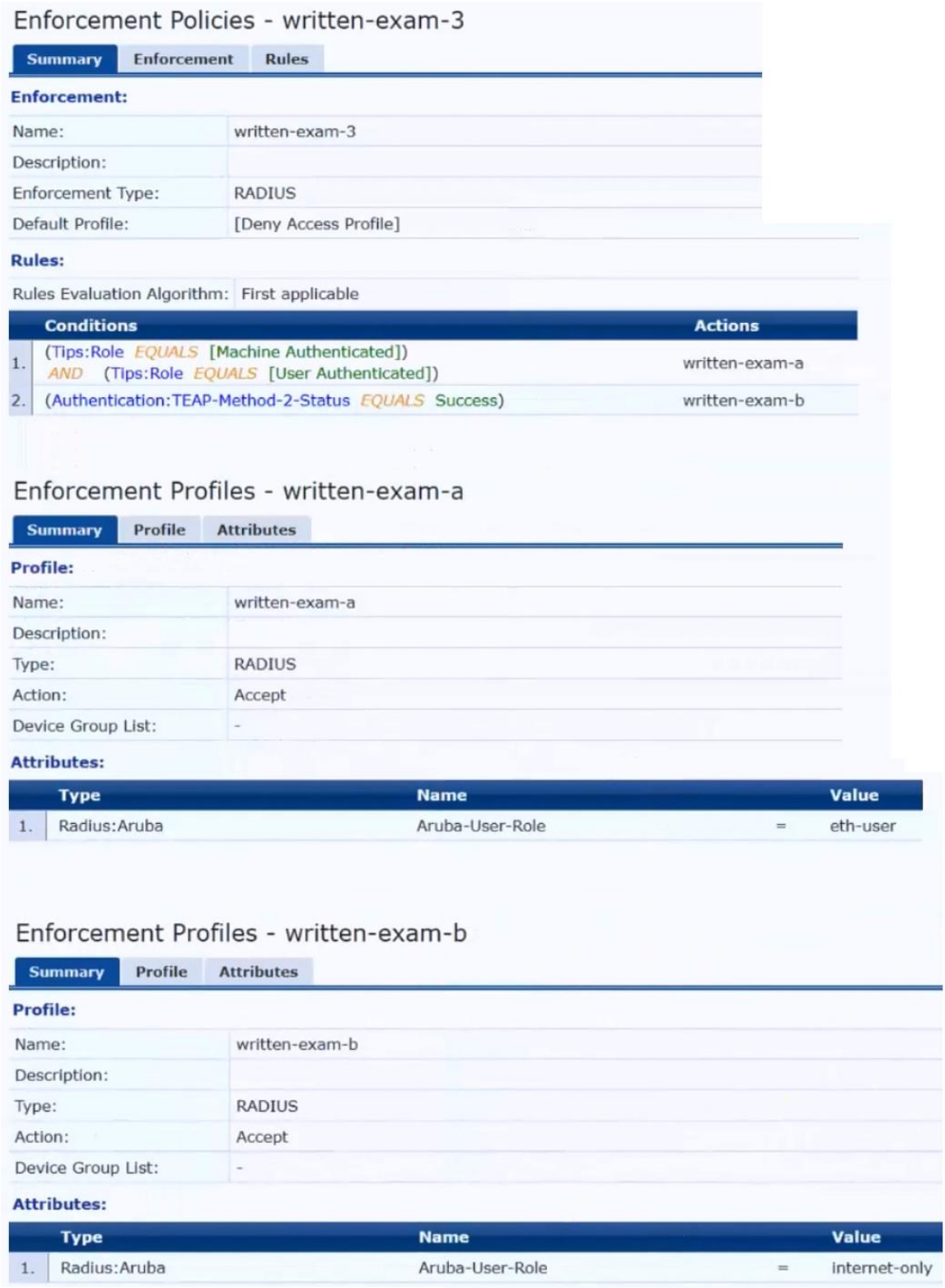
Answer: A
Explanation:
This option allows CPPM to receive real-time information about the network activity and security posture of the clients from the firewall, and then apply appropriate enforcement actions based on the configured policies. For example, if a client is detected to be infected with malware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

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	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
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. 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. The IP addresses of the gateways should be their system IP addresses, which are used for inter-controller communication and cluster discovery.
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. 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.
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.

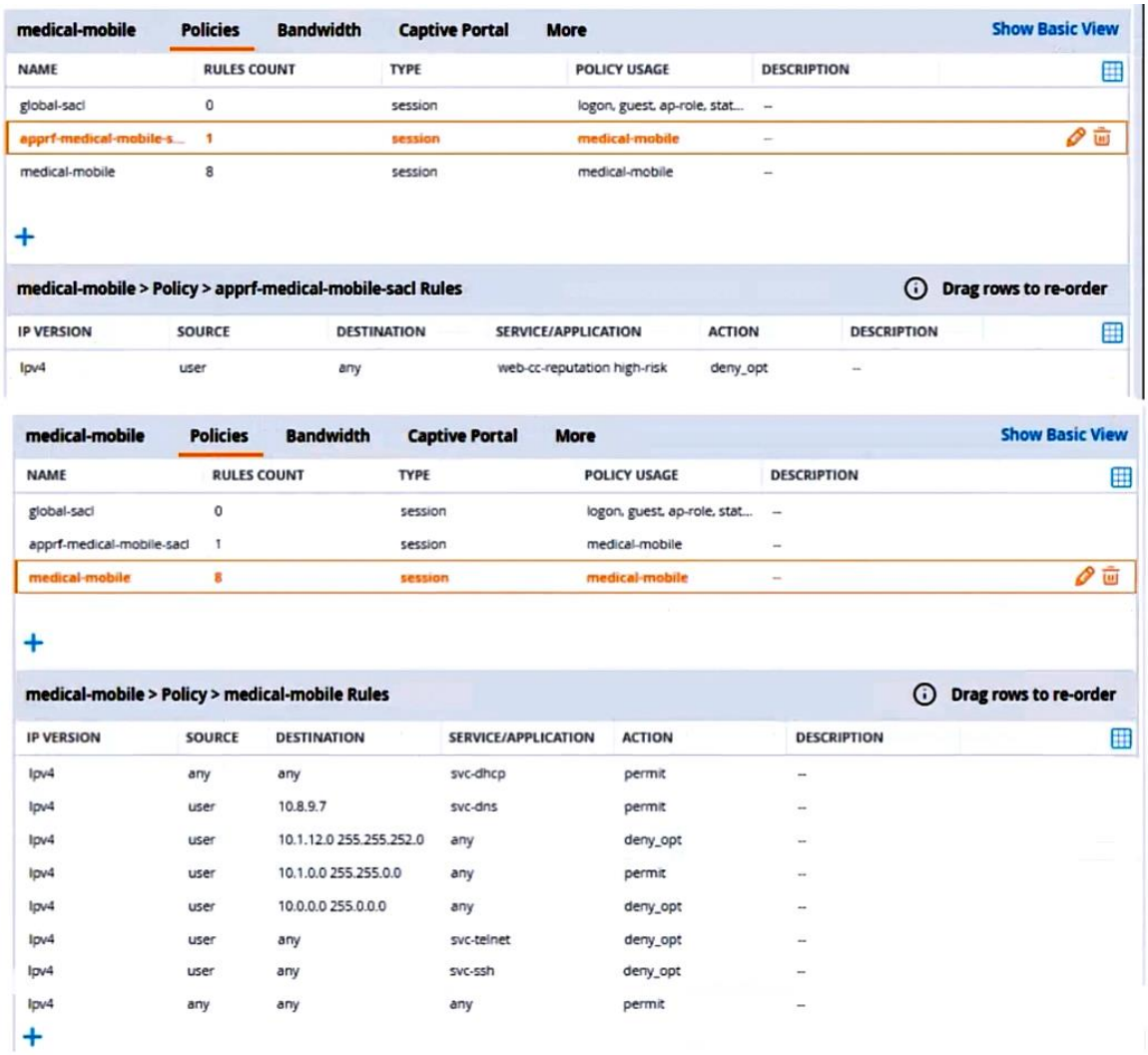
QUESTION 3
Refer to the scenario. A customer requires these rights for clients in the "medical-mobile" AOS firewall role on Aruba Mobility Controllers (MCs):

```
- 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.

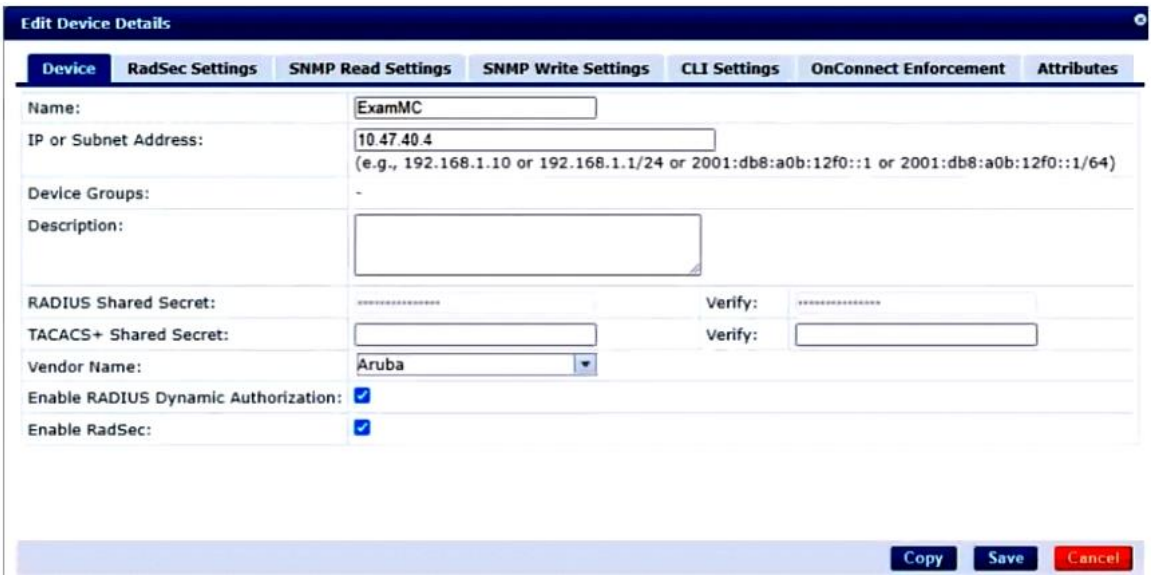


There are multiple issues with this configuration. What is one change you must make to meet the scenario requirements? (In the options, rules in a policy are referenced from top to bottom. For example, "medical-mobile" rule 1 is "ipv4 any any svc-dhcp permit," and rule 8 is "ipv4 any any any permit".)

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. 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. 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?

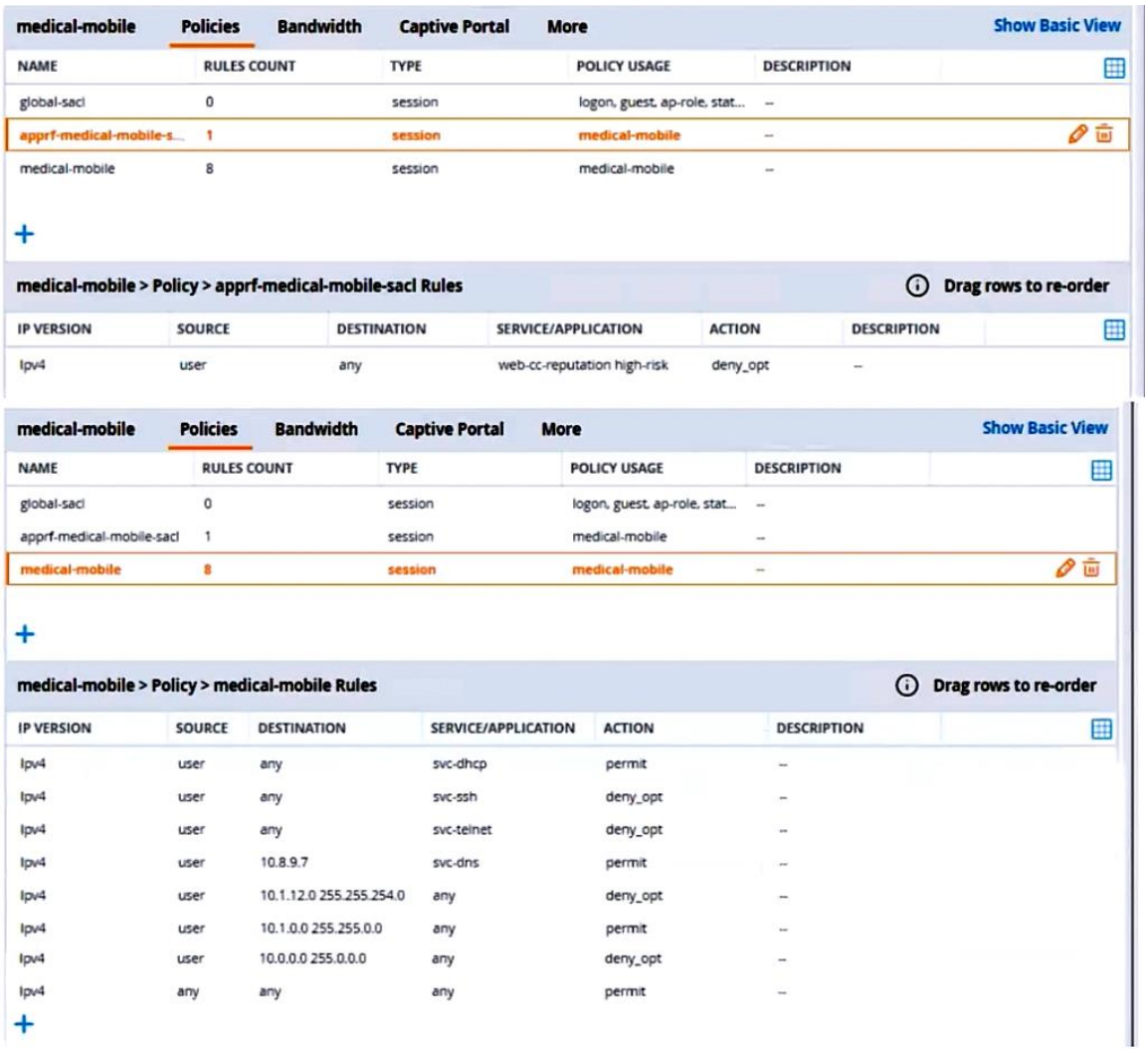
A. Change the UDP port in the MCs' RFC 3576 server config to 3799.
B. Enable RadSec on the MCs' RFC 3676 server config.
C. Configure the MC to obtain the time from a valid NTP server.
D. Make sure that CPPM is using an ArubaOS Wireless RADIUS CoA enforcement profile.

Answer: B
Explanation:
When you define RFC 3576 server you define IP address and shared key. The default value is UDP port 3799.
RADSEC (Secure RADIUS) auth port 2083 and it used Certificates.
When the TLS tunnel is established, RADIUS packets will go through the tunnel and server adds CoA on this tunnel.
By default, the TCP port 2083 is assigned for RadSec. Separate ports are not used for authentication, accounting and dynamic authorization changes.

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 | 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

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. 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. 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 >

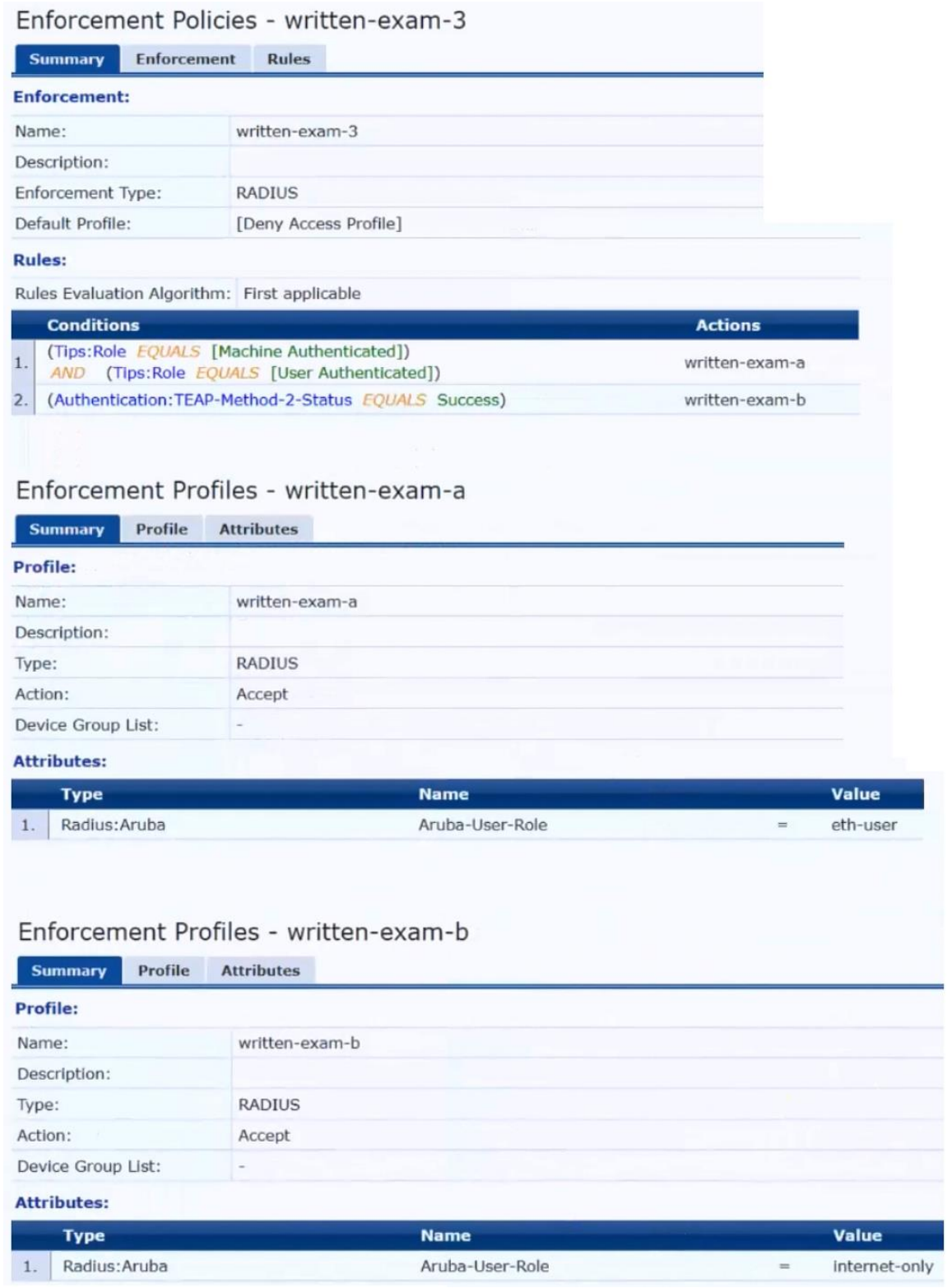
WebCC, respectively.
You also need to make sure that the MCs have valid licenses for AppRF and WebCC, which are included in the ArubaOS PEFNG license.

QUESTION 6
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
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.

Assume that you have configured the correct UBT zone and port-access role settings. However, the solution is not working.

What else should you make sure to do?

A. Assign VLAN 20 as the access VLAN on any edge ports to which tunneled clients might connect.
B. Create a new VLAN on the AOS-CX switch and configure that VLAN as the UBT client VLAN.
C. Assign sufficient VIA licenses to the gateways based on the number of wired clients that will connect.
D. Change the port-access auth-mode mode to client-mode on any edge ports to which tunneled clients might connect.

Answer: B
Explanation:
The correct answer is B. Create a new VLAN on the AOS-CX switch and configure that VLAN as the UBT client VLAN.
User-based tunneling (UBT) is a feature that allows the AOS-CX switches to tunnel the traffic from wired clients to a mobility gateway cluster, where they can be assigned a role and a VLAN based on their authentication and authorization. To enable UBT, the switches need to have a UBT zone configured with the IP addresses of the gateways, and a UBT client VLAN configured with the ubt- client-vlan command.
The UBT client VLAN is a special VLAN that is used to encapsulate the traffic from the tunneled clients before sending it to the gateways. The UBT client VLAN must be different from any other VLANs used on the switch or the network, and it must not be assigned to any ports or interfaces on the switch. The UBT client VLAN is only used internally by the switch for UBT, and it is not visible to the clients or the gateways.
In this scenario, the customer wants to tunnel the clients that pass user authentication to the gateway cluster, where they will be assigned to VLAN 20. Therefore, the switch must have a UBT client VLAN configured that is different from VLAN 20 or any other VLANs on the network. For example, the switch can use VLAN 4000 as the UBT client VLAN, as shown in one of the web search results. The switch must also have a UBT zone configured with the system IP addresses of the gateways as the primary and backup controllers, as explained in question.

QUESTION 7
A company has Aruba gateways and wants to start implementing gateway IDS/IPS. The customer has selected Block for the Fail Strategy.
What might you recommend to help minimize unexpected outages caused by using this particular fall strategy?

A. Configuring a relatively high threshold for the gateway threat count alerts
B. Making sure that the gateways have formed a cluster and operate in default gateway mode
C. Setting the IDS or IPS policy to the least restrictive option, Lenient
D. Enabling alerts and email notifications for events related to gateway IPS engine utilization and errors

Answer: D
Explanation:
Gateway IDS/IPS is a feature that allows the Aruba gateways to monitor and block malicious or unwanted traffic based on predefined or custom rules. The Fail Strategy is a setting that determines how the gateways handle traffic when the IPS engine fails or crashes. The Block option means that the gateways will stop forwarding traffic until the IPS engine recovers, while the Bypass option means that the gateways will continue forwarding traffic without inspection. The Block option provides more security, but it also increases the risk of network outages if the IPS engine fails frequently or for a long time. To minimize this risk, it is recommended to enable alerts and email notifications for events related to gateway IPS engine utilization and errors. This way, the network administrators can be informed of any issues with the IPS engine and take appropriate actions to restore or troubleshoot it.

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.lead2pass.com/all-products.html

10% Discount Coupon Code: **ASTR14**