

Exam : HPE6-A84

Title:Aruba Certified NetworkSecurity Expert WrittenExam

Version : DEMO

The safer , easier way to help you pass any IT exams.

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 |
|-----------------|-------------|------------|
| Enforcement | t: | |
| Name: | v | ritten-exa |
| Description: | | |
| Enforcement | Type: R | ADIUS |
| Default Profile | e: [| Deny Acce |

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:

| | Туре | 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 L | ist: | - | | | |
| Attributes: | | | | | |
| Туре | | | Name | | Value |
| 1. Radius:Ar | uba | | 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.

| global-saci 0 session logon, guest, ap-role, stat apprf*medical-mobile 8 session medical-mobile - medical-mobile > Policies Bandwidth Captive Portal More PVERSION SOURCE DESTINATION SERVICE/APPLICATION ACTION DESCRIPTION pv4 user any web-cc-reputation high-risk deny_opt medical-mobile Policies Bandwidth Captive Portal More Show Basic Vie NAME RULES COUNT TYPE POLICY USAGE DESCRIPTION global-saci 1 session medical-mobile - medical-mobile 4 session medical-mobile - pv4 session medical-mobile - medical-mobile sed 1 session medical-mobile - pv4 session medical-mobile - pv4 session medical-mobile - pv4 session medical-mobile - medical-mobile sed 1 session medical-mobile - pv4 sessin - pv4 sessin - pv4 session medical-mobile | | Policies | Bandwidth | Captive Portal | More | | | | Show Basic View |
|--|--|--|--|--|---|-----------|------------|---------|-----------------------|
| apperf medical-mabile s1 session medical-mobile - | NAME | RULES | COUNT 1 | YPE | POLICY USAGE | | ESCRIPTION | | [|
| medical-mobile 8 session medical-mobile | global-saci | 0 | | session | logon, guest, ap-ro | ole, stat | - | | |
| Imaginal mobile > Policy > apprf-medical-mobile-sacl Rules Imaginal mobile > Rules DESTRINATION SERVICE/APPLICATION ACTION DESCRIPTION Escription Ipv4 user any web-cc-reputation high-risk deny_opt – Show Basic Vie NAME RULES COUNT TYPE POLICY USAGE DESCRIPTION E agorf-medical-mobile 0 session logon, guest, ap-role, stat – agorf-medical-mobile 1 session medical-mobile – medical-mobile 0 session medical-mobile – medical-mobile 1 session medical-mobile – medical-mobile 0 session medical-mobile – medical-mobile 1 session medical-mobile – medical-mobile 0 session medical-mobile – medical-mobile > Policy > medical-mobile – Policy Policy medical-mobile 0 session medical-mobile – medical-mobile > Policy > medical-mobile – – Policy Policy | apprf-medical-mobile | HS 1 | | ession | medical-mobile | | - | | Ø 🗊 |
| Image: Coll-or > apprf-medical-mobile-sact Rules Image: Coll or Policy > any SERVICE/APPLICATION ACTION DESCRIPTION ESCRIPTION | medical-mobile | 8 | 1 | ession | medical-mobile | | - | | |
| P 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 Vie NAME RULES COUNT TYPE POLICY USAGE DESCRIPTION E global-saci 0 session logon, guest, ap-role, stat - apprf-medical-mobile 1 session medical-mobile - medical-mobile 8 session medical-mobile - P VERSION SOURCE DESTINATION SERVICE/APPLICATION ACTION DESCRIPTION Ipv4 any any svc.dhcp permit - 2000 Ipv4 user 10.0.0.255.255.252.0 any deny_opt - - Ipv4 user 10.0.0.255.0.0.0 any permit - - - Ipv4 user any svc.dhcp permit - - - - Ipv4 user <td>÷</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> | ÷ | | | | | | | | |
| Ipp4 user any web-cc-reputation high-risk deny_opt - Imedical-mobile Policies Bandwidth Captive Portal More | medical-mobile > F | Policy > appr | f-medical-mobile-s | acl Rules | | | | 0 | Drag rows to re-order |
| medical-mobile Policies Bandwidth Captive Portal More Show Basic View NAME RULES COUNT TYPE POLICY USAGE DESCRIPTION []] gjobal-saci 0 session logon, guest, ap-role, stat – apprf-medical-mobile 1 session medical-mobile – medical-mobile 8 session medical-mobile – medical-mobile 8 session medical-mobile – medical-mobile 8 session medical-mobile – ? ? ? medical-mobile 8 session medical-mobile – ? ? ? medical-mobile 8 session medical-mobile – ? ? ? medical-mobile > Policy > medical-mobile Rules session medical-mobile – ? ? ? ? IP VERSION SOURCE DESTINATION SERVICE/APPLICATION ACTION DESCRIPTION ? Ipv4 user 101.12.0 255.255.252.0 any deny_opt – <th< td=""><td>PVERSION</td><td>SOURCE</td><td>DESTINA</td><td>TION SE</td><td>RVICE/APPLICATION</td><td>ACTION</td><td>DESC</td><td>RIPTION</td><td></td></th<> | PVERSION | SOURCE | DESTINA | TION SE | RVICE/APPLICATION | ACTION | DESC | RIPTION | |
| NAME RULES COUNT TYPE POLICY USAGE DESCRIPTION E global-saci 0 session logon, guest. ap-role, stat – apprf-medical-mobile-saci 1 session medical-mobile – medical-mobile 8 session medical-mobile – medical-mobile Policy > medical-mobile Rules medical-mobile – IP VERSION SOURCE DESTINATION SERVICE/APPLICATION ACTION DESCRIPTION Image: Comparison of the policy of the polic | lpv4 | user | any | W | eb-cc-reputation high-risk | deny_opt | - | | |
| global-saci 0 session logon, guest, ap-role, stat - apprf-medical-mobile 1 session medical-mobile - medical-mobile 6 session medical-mobile - medical-mobile 6 session medical-mobile - <t< td=""><td>medical-mobile</td><td>Policies</td><td>Bandwidth</td><td>Captive Portal</td><td>More</td><td></td><td></td><td></td><td>Show Basic Vie</td></t<> | medical-mobile | Policies | Bandwidth | Captive Portal | More | | | | Show Basic Vie |
| apprf-medical-mobile-sad 1 session medical-mobile - medical-mobile 6 session medical-mobile - medical-mobile 8 session medical-mobile - <th< td=""><td>NAME</td><td>RULES C</td><td>COUNT 1</td><td>YPE</td><td>POLICY USAGE</td><td></td><td>ESCRIPTION</td><td></td><td>(</td></th<> | NAME | RULES C | COUNT 1 | YPE | POLICY USAGE | | ESCRIPTION | | (|
| session medical-mobile - P | giobal-saci | 0 | : | session | logon, guest, ap-ro | ole, stat | - | | |
| IP VERSION SOURCE DESTINATION SERVICE/APPLICATION ACTION DESCRIPTION Drag rows to re-order Ipv4 any any any svc-dhcp permit - Ipv4 user 10.8.9.7 svc-dns permit - Ipv4 user 10.1.12.0.255.255.25.0 any deny_opt - Ipv4 user 10.1.0.0.255.255.0.0 any permit - Ipv4 user 10.1.0.0.255.255.0.0 any deny_opt - Ipv4 user 10.0.0.255.0.0.0 any deny_opt - Ipv4 user any svc-teinet deny_opt - | apprf-medical-mobile- | saci 1 | | session | medical-mobile | | - | | |
| IP VERSION SOURCE DESTINATION SERVICE/APPLICATION ACTION DESCRIPTION DESCRIPTION Ipv4 any any svc-dhcp permit - | | | | | | | | | 0- |
| Ipv4 any any svc-dhcp permit Ipv4 user 10.8.9.7 svc-dns permit Ipv4 user 10.1.12.0.255.255.25.0 any deny_opt Ipv4 user 10.1.0.0.255.255.0.0 any permit Ipv4 user 10.0.0.255.0.0.0 any permit Ipv4 user 10.0.0.255.0.0.0 any deny_opt Ipv4 user any svc-teinet deny_opt Ipv4 user any svc-teinet deny_opt Ipv4 user any svc-teinet deny_opt | medical-mobile | | | ession | medical-mobile | | | | Ø U |
| Ipv4 user 10.8.9.7 svc-dns permit - Ipv4 user 10.1.12.0.255.255.0 any deny_opt - Ipv4 user 10.1.0.0.255.255.00 any permit - Ipv4 user 10.1.0.0.255.255.00 any permit - Ipv4 user 10.0.0.255.00.0 any deny_opt - Ipv4 user any svc-teinet deny_opt - Ipv4 user any svc-teinet deny_opt - Ipv4 user any svc-teinet deny_opt - | + medical-mobile > F | Policy > medi | cal-mobile Rules | | | | | 0 | Drag rows to re-order |
| 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 10.0.0 255.0.0.0 any deny_opt Ipv4 user 10.0.0.0 255.0.0.0 any deny_opt Ipv4 user any svc-teinet deny_opt Ipv4 user any svc-teinet deny_opt Ipv4 user any svc-teinet deny_opt | medical-mobile > F version | Policy > medi SOURCE | cal-mobile Rules | SERVICE/AI | PPLICATION ACTION | | | 0 | |
| 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-telnet deny_opt Ipv4 user any svc-telnet deny_opt | medical-mobile > F P VERSION Ipv4 | Policy > medi SOURCE any | cal-mobile Rules DESTINATION any | SERVICE/AI svc-dhcp | PLICATION ACTION | | | 0 | Drag rows to re-order |
| lpv4 user 10.0.0.0 255.0.0.0 any deny_opt lpv4 user any svc-teinet deny_opt lpv4 user any svc-ssh deny_opt | P VERSION | Policy > medi SOURCE any user | cal-mobile Rules DESTINATION any 10.8.9.7 | SERVICE/AI svc-dhcp svc-dns | PPLICATION ACTION permit permit | | | 0 | Drag rows to re-order |
| lpv4 user any svc-teinet deny_opt lpv4 user any svc-ssh deny_opt | P VERSION Ipv4 Ipv4 Ipv4 Ipv4 | Policy > medi SOURCE any user user | cal-mobile Rules DESTINATION any 10.8.9.7 10.1.12.0 255.255.25 | SERVICE/AI svc-dhcp svc-dns 2.0 any | PPLICATION ACTION permit permit deny_opt | - | | 0 | Drag rows to re-order |
| Ipv4 user any svc-ssh deny_opt – | P VERSION PV4 Ipv4 Ipv4 Ipv4 Ipv4 | Policy > medi SOURCE any user user user user | cal-mobile Rules DESTINATION any 10.8.9.7 10.1.12.0 255.255.25 10.1.0.0 255.255.0.0 | SERVICE/AI svc-dhcp svc-dns 2.0 any any | PPLICATION ACTION permit permit deny_opt permit | | | Ō | Drag rows to re-order |
| | P VERSION IPV4 Ipv4 Ipv4 Ipv4 Ipv4 Ipv4 Ipv4 Ipv4 Ipv | Policy > medi SOURCE any user user user user user user | cal-mobile Rules DESTINATION any 10.8.9.7 10.1.12.0 255.255.25 10.1.0.0 255.255.0.0 10.0.0.0 255.0.0 | SERVICE/AI svc-dhcp svc-dns 2.0 any any any | PPLICATION ACTION permit permit deny_opt permit deny_opt | | | 0 | Drag rows to re-order |
| | P VERSION PVERSION Ipv4 Ipv4 Ipv4 Ipv4 Ipv4 Ipv4 Ipv4 Ipv4 | Policy > medi SOURCE any user user user user user user | cal-mobile Rules DESTINATION any 10.8.9.7 10.1.12.0 255.255.25 10.1.0.0 255.255.00 10.0.0.0 255.0.0 any | SERVICE/AI svc-dhcp svc-dns 2.0 any any any svc-teinet | PPLICATION ACTION permit permit deny_opt permit deny_opt deny_opt | | | 0 | Drag rows to re-order |

+

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).

Copy Save Cancel

| Device RadSec Settings | SNMP Read Settings | SNMP Write Settings | CLI Settings | OnConnect Enforcement | Attributes |
|---|--------------------|--------------------------|---------------|------------------------------|-------------|
| Name: | ExamMC | | | | |
| IP or Subnet Address: | 10.47.40.4 | | | | |
| | (e.g., 192.168 | 8.1.10 or 192.168.1.1/24 | or 2001:db8:a | 0b:12f0::1 or 2001:db8:a0b: | 12f0::1/64) |
| Device Groups: | - | | | | |
| Description: | | | | | |
| | | | | | |
| RADIUS Shared Secret: | | | Verify: | | |
| | | | | | - |
| | | | veniy: | | |
| | | • | | | |
| Enable RADIUS Dynamic Autho | rization: 🗹 | | | | |
| | a | | | | |
| TACACS+ Shared Secret: Vendor Name: Enable RADIUS Dynamic Autho | | ▼ | Verify: | | |

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 Invalid Req | | q Disconnect Acc Unknown service | | - | | Bad Auth |
|-----------------------|---|-------------------------------------|-----|---|---|----------|
| | | | | | | |
| | | | | | | |
| 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.

| medical-mobile | Policies | Bandwidth | Captive Portal | More | | | Show Basic View |
|---|--|---|--|---|--------------|-------------|-----------------------|
| NAME | RULES | COUNT | ТҮРЕ | POLICY USAGE | DESCRIPTI | ON | E |
| global-saci | 0 | | session | logon, guest, ap- | role, stat – | | |
| apprf-medical-mobil | le-s 1 | | session | medical-mobile | - | | Ø 🗊 |
| medical-mobile | 8 | | session | medical-mobile | - | | |
| F | | | | | | | |
| medical-mobile > 1 | Policy > appr | f-medical-mobile- | saci Rules | | | 0 | Drag rows to re-order |
| P VERSION | SOURCE | DESTINA | ATION SERV | ICE/APPLICATION | ACTION | DESCRIPTION | • |
| lpv4 | user | any | web- | cc-reputation high-risk | deny_opt | - | |
| medical-mobile | Policies | Bandwidth | Captive Portal | More | | | Show Basic View |
| NAME | RULES | COUNT | ТҮРЕ | POLICY USAGE | DESCRIPTIO | N | E |
| global-saci | 0 | | session | logon, guest, ap-ro | ole, stat | | |
| apprf-medical-mobile- | -sacl 1 | | session | medical-mobile | - | | |
| medical-mobile | 8 | | session | | | | - A |
| | | | ac a second | medical-mobile | - | | Ø 🔟 |
| + | Later, | | | medical-mobile | | | 6 1 |
| + medical-mobile > I | Policy > med | | | medical-mobile | - | Ō | |
| nedical-mobile > I | Policy > med | | SERVICE/APPLI | | DESCRIP | Ŭ | Drag rows to re-order |
| nedical-mobile > I P VERSION | - | ical-mobile Rules | | | | Ŭ | |
| nedical-mobile > I P VERSION | SOURCE | ical-mobile Rules | SERVICE/APPLI | CATION ACTION | DESCRIP | Ŭ | Drag rows to re-order |
| nedical-mobile > I P VERSION Ipv4 Ipv4 | SOURCE | ical-mobile Rules DESTINATION any | SERVICE/APPLI svc-dhcp | CATION ACTION | DESCRIP | Ŭ | Drag rows to re-order |
| nedical-mobile > I P VERSION Ipv4 Ipv4 | SOURCE user user | any | SERVICE/APPLI svc-dhcp svc-ssh | CATION ACTION permit deny_opt | DESCRIP | Ŭ | Drag rows to re-order |
| medical-mobile > I P VERSION Ipv4 Ipv4 Ipv4 Ipv4 | SOURCE user user user | ical-mobile Rules DESTINATION any any any | SERVICE/APPLI svc-dhcp svc-ssh svc-teinet svc-dns | CATION ACTION permit deny_opt deny_opt | DESCRIP | Ŭ | Drag rows to re-order |
| nedical-mobile > I P VERSION Ipv4 Ipv4 Ipv4 Ipv4 Ipv4 | SOURCE user user user user | ical-mobile Rules DESTINATION any any any 10.8.9.7 | SERVICE/APPLI svc-dhcp svc-ssh svc-teinet svc-dns | CATION ACTION permit deny_opt deny_opt permit | DESCRIP | Ŭ | Drag rows to re-order |
| P VERSION PVERSION PVERSION pv4 | SOURCE user user user user user | any any any any 10.8.9.7 | SERVICE/APPLI Svc-dhcp svc-ssh svc-teinet svc-dns 4.0 any | CATION ACTION permit deny_opt deny_opt permit deny_opt | DESCRIP | Ŭ | Drag rows to re-order |

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