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

Aruba Certified Network Security Expert Written

Pass HP HPE6-A84 Exam with 100% Guarantee

QUESTION 1

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.

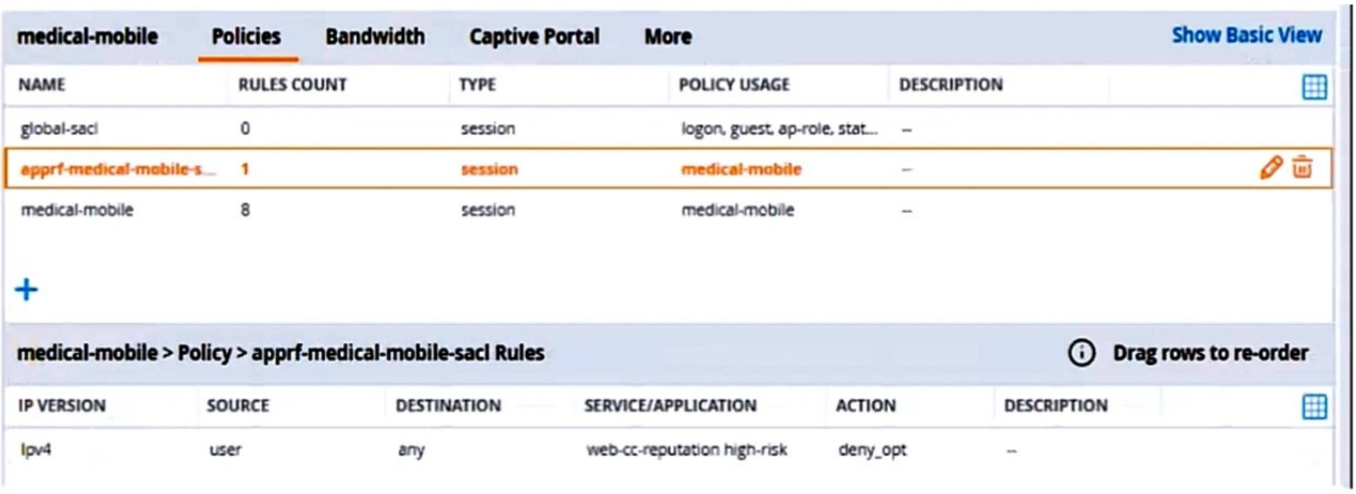
Denied access to the WLAN for a period of time if they send any Telnet traffic

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.

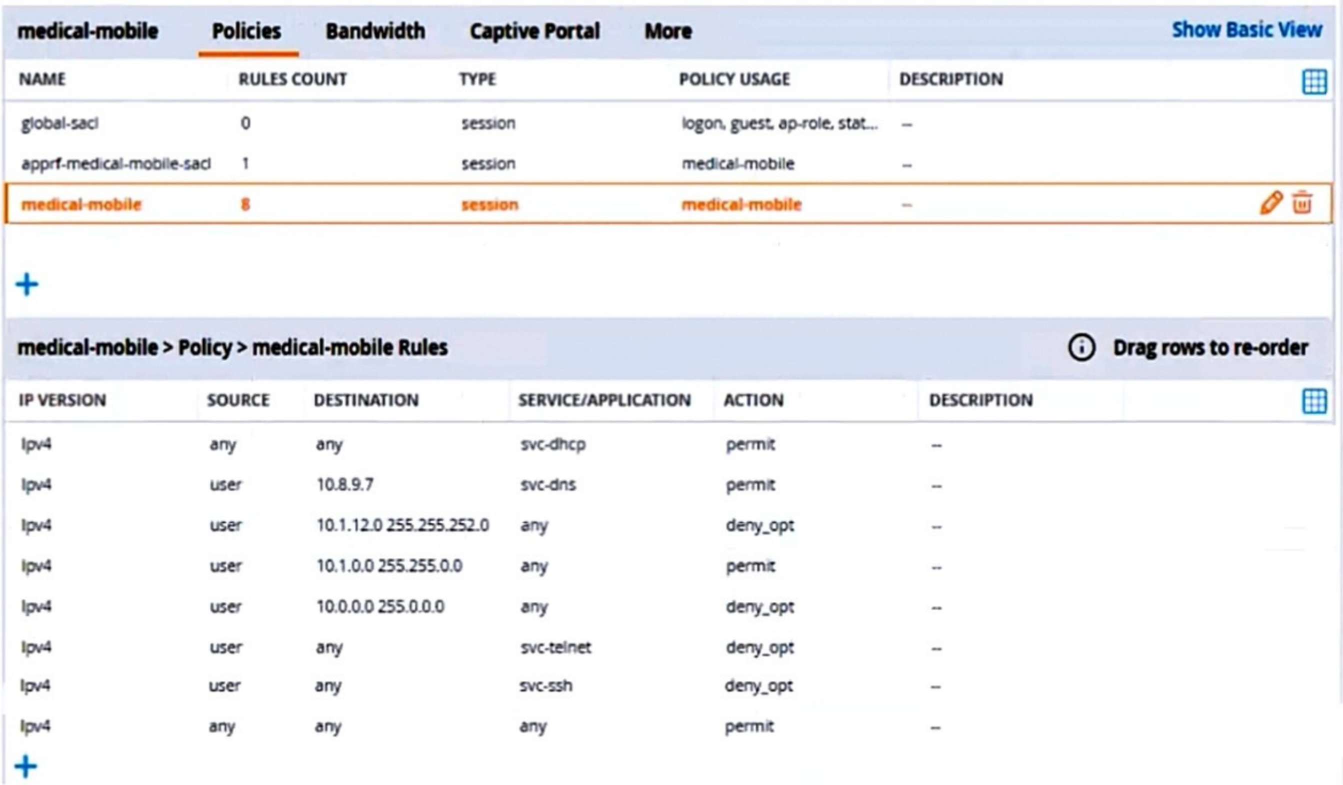


NAME	RULES COUNT	TYPE	POLICY USAGE	DESCRIPTION
global-sacl	0	session	logon, guest, ap-role, stat...	--
apprf-medical-mobile-s...	1	session	medical-mobile	--
medical-mobile	8	session	medical-mobile	--

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	--



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."

Correct Answer: B

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 2

The customer needs a way for users to enroll new wired clients in Intune. The clients should have limited access that only lets them enroll and receive certificates. You plan to set up these rights in an AOS-CX role named "provision."

The customer\\'s security team dictates that you must limit these clients\\' Internet access to only the necessary sites. Your switch software supports IPv4 and IPv6 addresses for the rules applied in the "provision" role.

What should you recommend?

A. Configuring the rules for the "provision" role with IPv6 addresses, which tend to be more stable

B. Enabling tunneling to the MCs on the "provision" role and then setting up the privileges on the MCs

C. Configuring the "provision" role as a downloadable user role (DUR) in CPPM

D. Assigning the "provision" role to a VLAN and then setting up the rules within a Layer 2 access control list (ACL)

Correct Answer: C

This is because a downloadable user role (DUR) is a feature that allows the switch to use a central ClearPass server to download user-roles to the switch for authenticated users12 A DUR can contain various attributes and rules that define the access level and privileges of the user, such as VLAN, ACL, PoE, reauthentication period, etc3 A DUR can also be customized and updated on the ClearPass server without requiring any changes on the switch1 A DUR can be used to create a "provision" role that allows users to enroll new wired clients in Intune. The "provision" role can have limited access that only lets them enroll and receive certificates from the Intune service. The "provision" role can also have rules that restrict the Internet access of the users to only the necessary sites, such as the Intune portal and the certificate authority. The rules can be based on IPv4 or IPv6 addresses, depending on the network configuration and preference2 A. Configuring the rules for the "provision" role with IPv6 addresses, which tend to be more stable. This is not a valid recommendation because it does not address how to create and apply the "provision" role on the switch. Moreover, IPv6 addresses do not necessarily tend to be more stable than IPv4 addresses, as both protocols have their own advantages and disadvantages4

B. Enabling tunneling to the MCs on the "provision" role and then setting up the privileges on the MCs. This is not a valid recommendation because it does not explain how to enable tunneling or what MCs are. Moreover, tunneling is a technique that encapsulates one network protocol within another, which adds complexity and overhead to the network communication5

D. Assigning the "provision" role to a VLAN and then setting up the rules within a Layer 2 access control list (ACL). This is not a valid recommendation because it does not explain how to assign a role to a VLAN or how to create a Layer 2 ACL on the switch. Moreover, a Layer 2 ACL is limited in its filtering capabilities, as it can only match on MAC addresses or Ethernet types, which might not be sufficient for restricting Internet access to specific sites

QUESTION 3

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

Correct Answer: A

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 4

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.

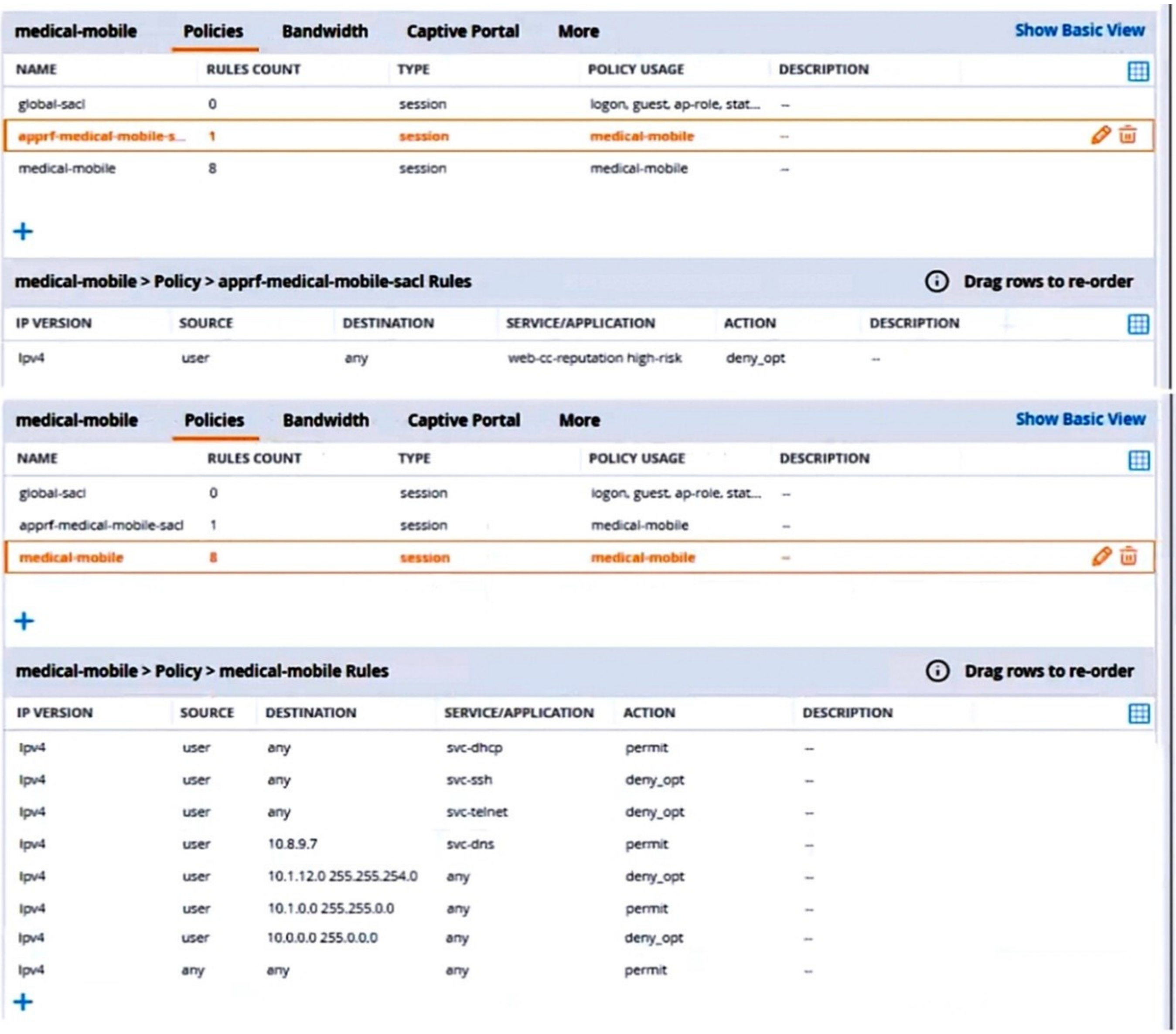
Denied access to the WLAN for a period of time if they send any Telnet traffic

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 line below shows the effective 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	--

+

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 6 is "ipv4 any any any permit\\'.)

A. Apply the "apprf-medical-mobile-sjcT policy explicitly to the \\'medical-mobile\\' user-role under the \\'medical-mobile" policy.

B. In the "medical-mobile" policy, change the action for rules 2 and 3 to reject.

C. In the "medical-mobile" policy, move rule 5 under rule 6.

D. In the "medical-mobile* policy, change the subnet mask in rule 5 to 255.255.252.0.

Correct Answer: D

The scenario requires that the clients in the "medical-mobile" role are denied access to the 10.1.12.0/22 subnet, which is a range of IP addresses from 10.1.12.0 to 10.1.15.255. However, the current configuration in rule 5 has a subnet mask of 255.255.240.0, which means that it matches any IP address from 10.1.0.0 to 10.1.15.255. This is too broad and would deny access to other subnets in the 10.1.0.0/16 range that should be permitted according to the scenario. Therefore, the subnet mask in rule 5 should be changed to 255.255.252.0, which would match only the IP addresses from 10.1.12.0 to 10.1.15.255 and deny access to them as required by the scenario

QUESTION 5

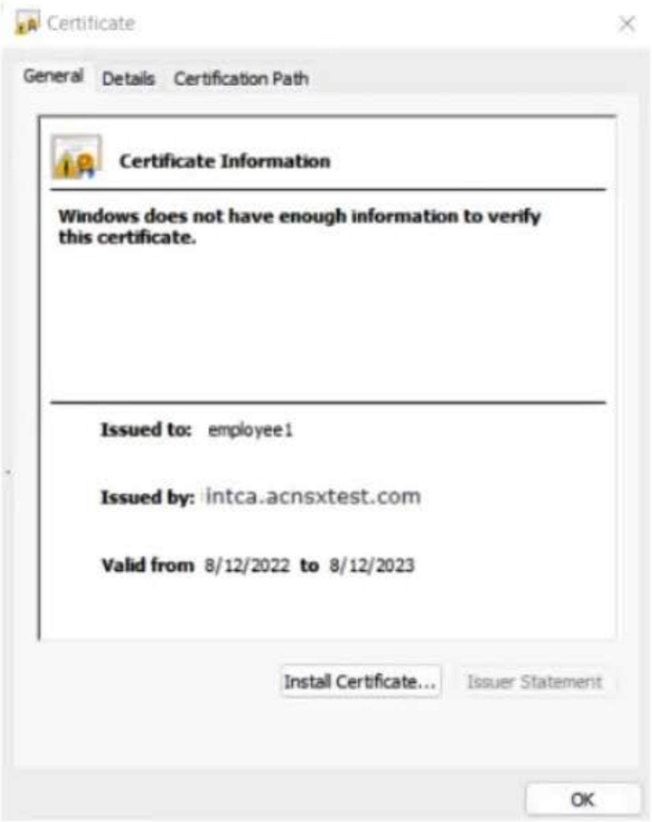
Refer to the scenario.

# Introduction to the customer

You are helping a company add Aruba ClearPass to their network, which uses Aruba network infrastructure devices.

The company currently has a Windows domain and Windows CA. The Window CA issues certificates to domain computers, domain users, and servers such as domain controllers. An example of a certificate issued by the Windows CA is

shown here.



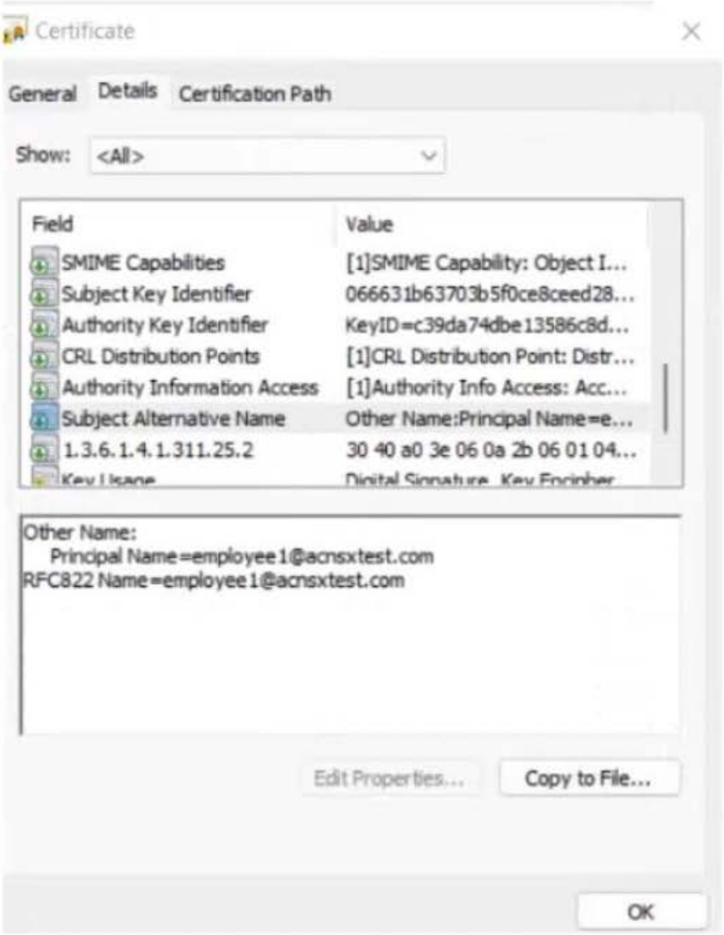
Certificate Information

Windows does not have enough information to verify this certificate.

Issued to: employee1

Issued by: intca.acnsxtest.com

Valid from 8/12/2022 to 8/12/2023



Show: <All>

Field	Value
SMIME Capabilities	[1]SMIME Capability: Object I...
Subject Key Identifier	066631b63703b5f0ce8ceed28...
Authority Key Identifier	KeyID=c39da74dbe13586c8d...
CRL Distribution Points	[1]CRL Distribution Point: Distr...
Authority Information Access	[1]Authority Info Access: Acc...
Subject Alternative Name	Other Name:Principal Name=e...
1.3.6.1.4.1.311.25.2	30 40 a0 3e 06 0a 2b 06 01 04...
Key Usage	Digital Signature, Key Encipher

```
Other Name:
    Principal Name=employee1@acnsxtest.com
RFC822 Name=employee1@acnsxtest.com
```

The company is in the process of adding Microsoft Endpoint Manager (Intune) to manage its mobile clients. The customer is maintaining the on-prem AD for now and uses Azure AD Connect to sync with Azure AD.

# Requirements for issuing certificates to mobile clients

The company wants to use ClearPass Onboard to deploy certificates automatically to mobile clients enrolled in Intune. During this process, Onboard should communicate with Azure AD to validate the clients. High availability should also be

provided for this scenario; in other words, clients should be able to get certificates from Subscriber 2 if Subscriber 1 is down.

The Intune admins intend to create certificate profiles that include a UPN SAN with the UPN of the user who enrolled the device.

# Requirements for authenticating clients

The customer requires all types of clients to connect and authenticate on the same corporate SSID.

The company wants CPPM to use these authentication methods:

1.

EAP-TLS to authenticate users on mobile clients registered in Intune

2.

TEAR, with EAP-TLS as the inner method to authenticate Windows domain computers and the users on them To succeed, EAP-TLS (standalone or as a TEAP method) clients must meet these requirements:

1.

Their certificate is valid and is not revoked, as validated by OCSP

2.

The client\\'s username matches an account in AD # Requirements for assigning clients to roles After authentication, the customer wants the CPPM to assign clients to ClearPass roles based on the following rules:

1.

Clients with certificates issued by Onboard are assigned the "mobile-onboarded" role

2.

Clients that have passed TEAP Method 1 are assigned the "domain-computer" role

3.

Clients in the AD group "Medical" are assigned the "medical-staff" role

4.

Clients in the AD group "Reception" are assigned to the "reception-staff" role The customer requires CPPM to assign authenticated clients to AOS firewall roles as follows:

1.

Assign medical staff on mobile-onboarded clients to the "medical-mobile" firewall role

2.

Assign other mobile-onboarded clients to the "mobile-other" firewall role

3.

Assign medical staff on domain computers to the "medical-domain" firewall role

4.

All reception staff on domain computers to the "reception-domain" firewall role

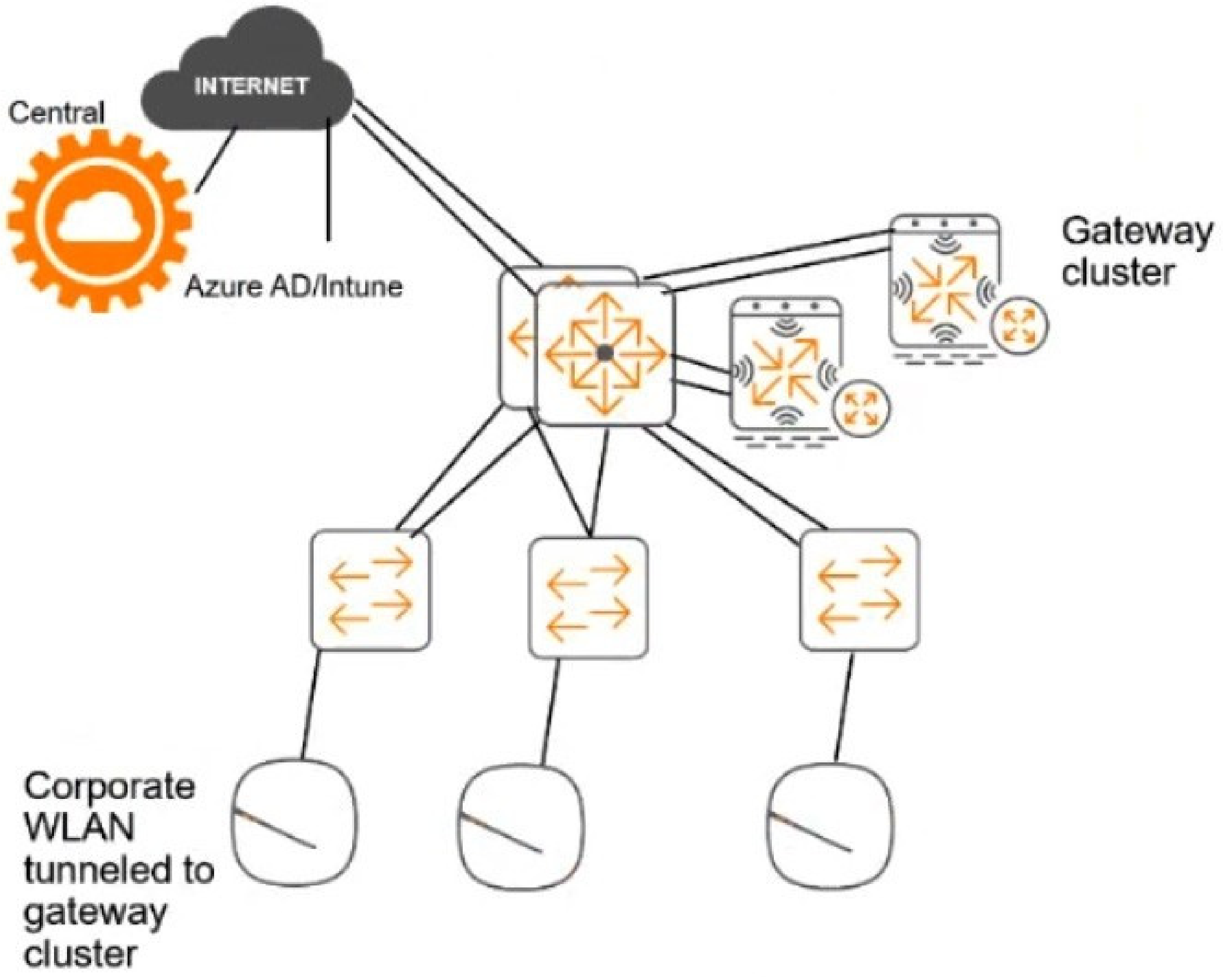
5.

All domain computers with no valid user logged in to the "computer-only" firewall role

6.

Deny other clients access # Other requirements Communications between ClearPass servers and on-prem AD domain controllers must be encrypted. # Network topology For the network infrastructure, this customer has Aruba APs and Aruba gateways, which are managed by Central. APs use tunneled WLANs, which tunnel traffic to the gateway cluster. The customer also has AOS-CX switches that are not

managed by Central at this point.



# ClearPass cluster IP addressing and hostnames

A customer\\'s ClearPass cluster has these IP addresses:

1.

Publisher = 10.47.47.5

2.

Subscriber 1 = 10.47.47.6

3.

Subscriber 2 = 10.47.47.7

4.

Virtual IP with Subscriber 1 and Subscriber 2 = 10.47.47.8

The customer\\'s DNS server has these entries

1.

cp.acnsxtest.com = 10.47.47.5

2.

cps1.acnsxtest.com = 10.47.47.6

3.

cps2.acnsxtest.com = 10.47.47.7

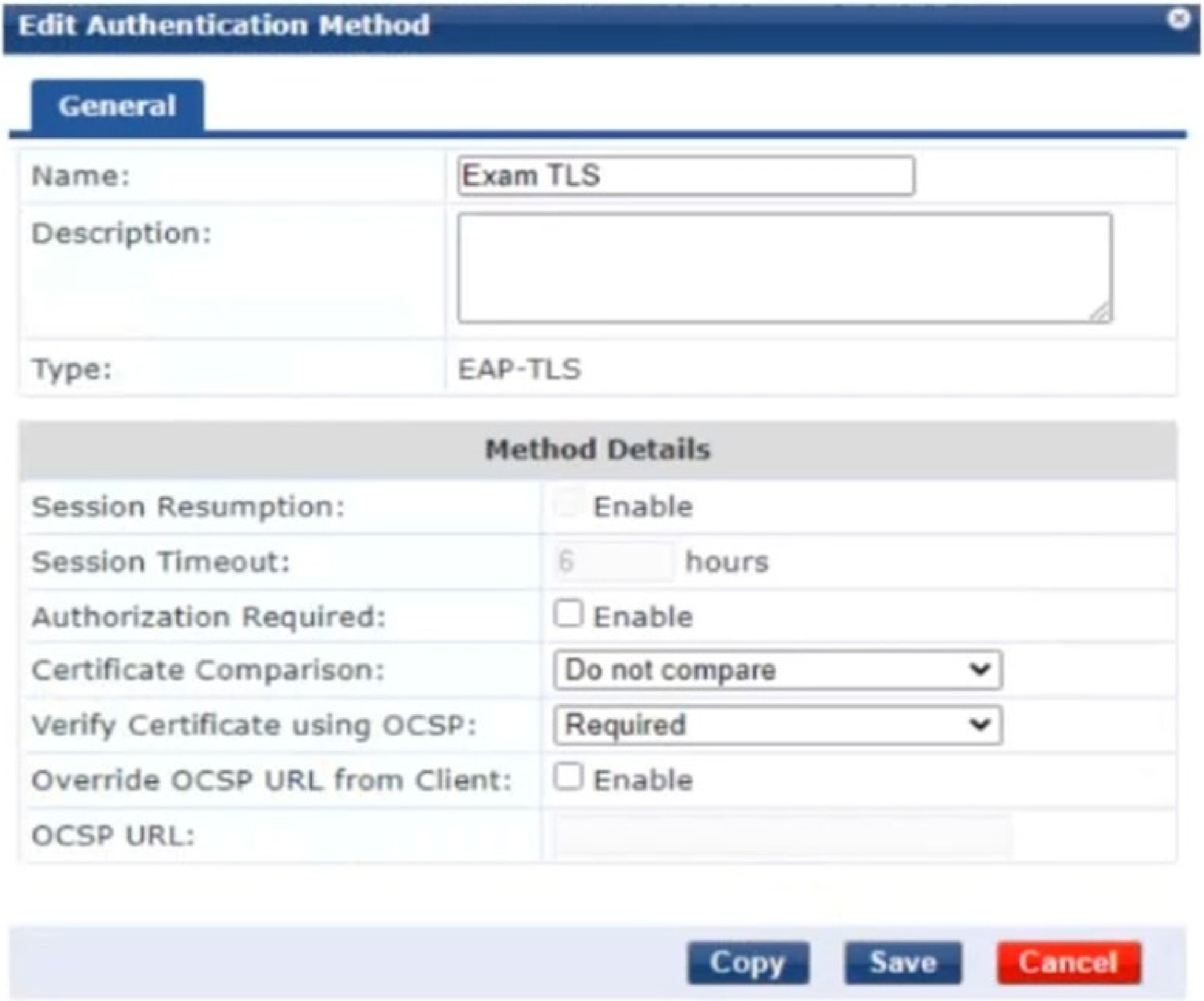
4.

radius.acnsxtest.com = 10.47.47.8

5.

onboard.acnsxtest.com = 10.47.47.8

On CPPM, you are creating the authentication method shown in the exhibit below:



Name:	Exam TLS
Description:	
Type:	EAP-TLS

Method Details

Session Resumption:	☐ Enable
Session Timeout:	6 hours
Authorization Required:	☐ Enable
Certificate Comparison:	Do not compare
Verify Certificate using OCSP:	Required
Override OCSP URL from Client:	☐ Enable
OCSP URL:	

You will use the method for standalone EAP-TLS and for inner methods in TEAP. What should you do?

A. Configure OCSP override and set the OCSP URL to localhost/onboard/mdps ocspphp/2

B. Enable certificate comparison.

C. Enable authorization.

D. Configure OCSP override and leave the OCSP URL blank.

Correct Answer: A