Vendor:HP

Exam Code:HPE6-A84

Exam Name: Aruba Certified Network Security Expert Written

Version: Demo

QUESTION 1

Refer to the scenario.

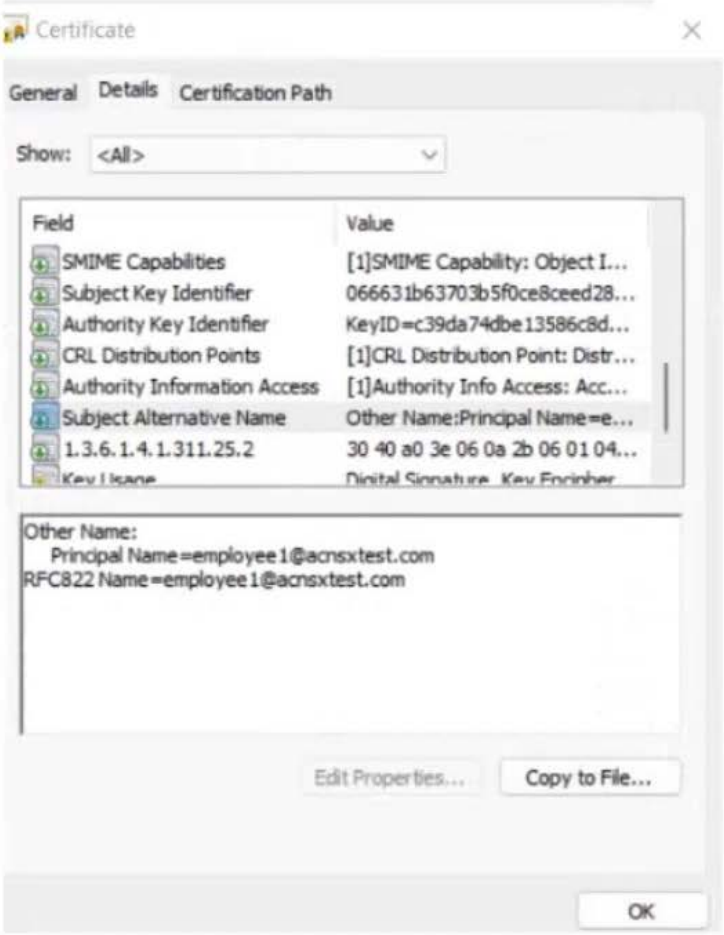
Introduction to the customer

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
General
Details
Certification Path
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
Install Certificate...
Issuer Statement
OK


Certificate
General
Details
Certification Path
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...
Other Name:
Principal Name=employee1@acnsxtest.com
RFC822 Name=employee1@acnsxtest.com
Edit Properties...
Copy to File...
OK

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

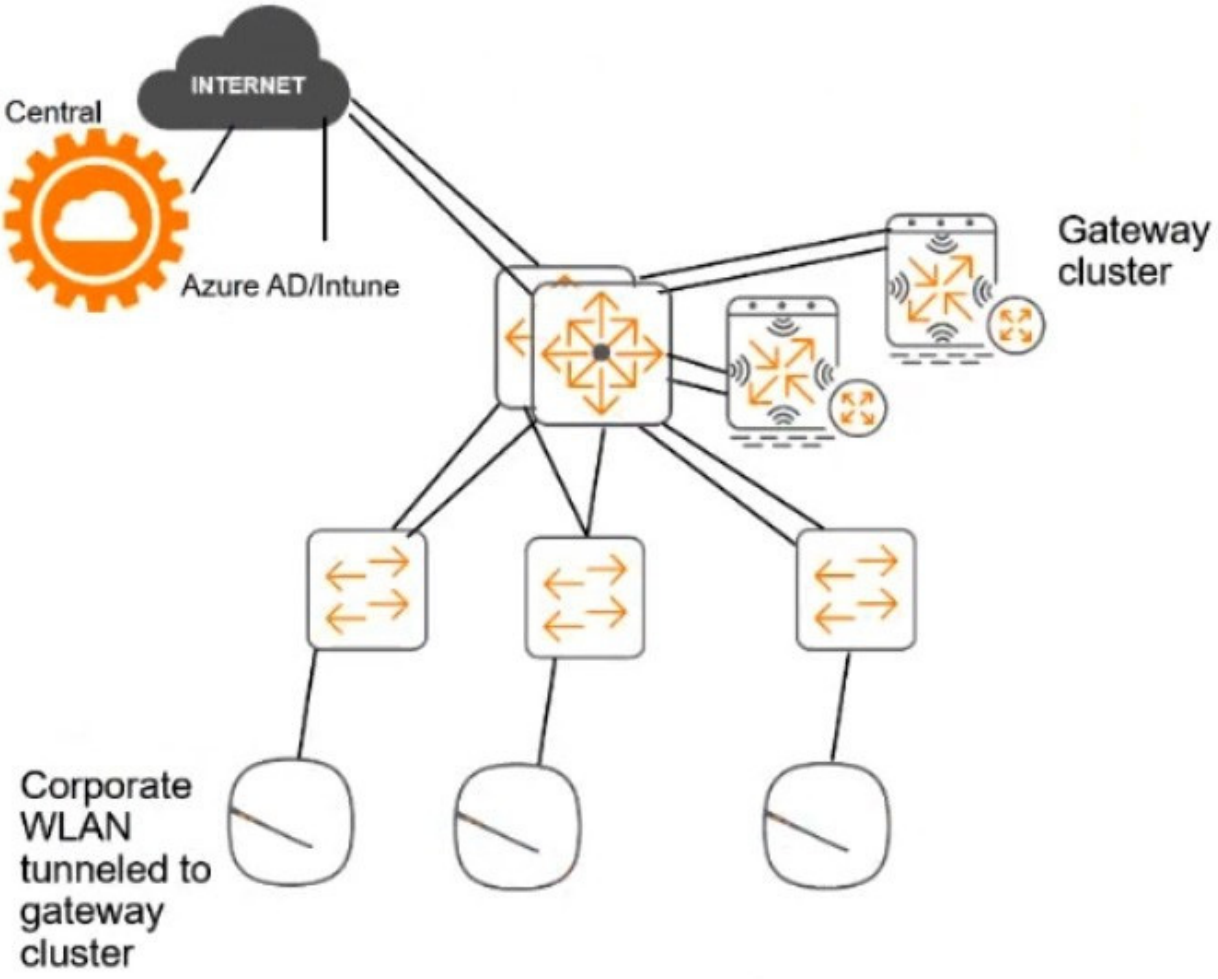
5.

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

The customer needs a secure way for users to enroll their new wireless clients in Intune. You are recommending a new WLAN that will provide the users with limited access for the enrollment.

You have set up captive portal for clients on this WLAN to a web page with instructions for enrolling devices. You will need to add several hostnames to the captive portal allowlist manually.

What is one of those hostnames?

A. The hostname used by ClearPass Policy ManaGer\\'s RADIUS services

B. The ClearPass Onboard hostname referenced in an Onboard provisioninG profile

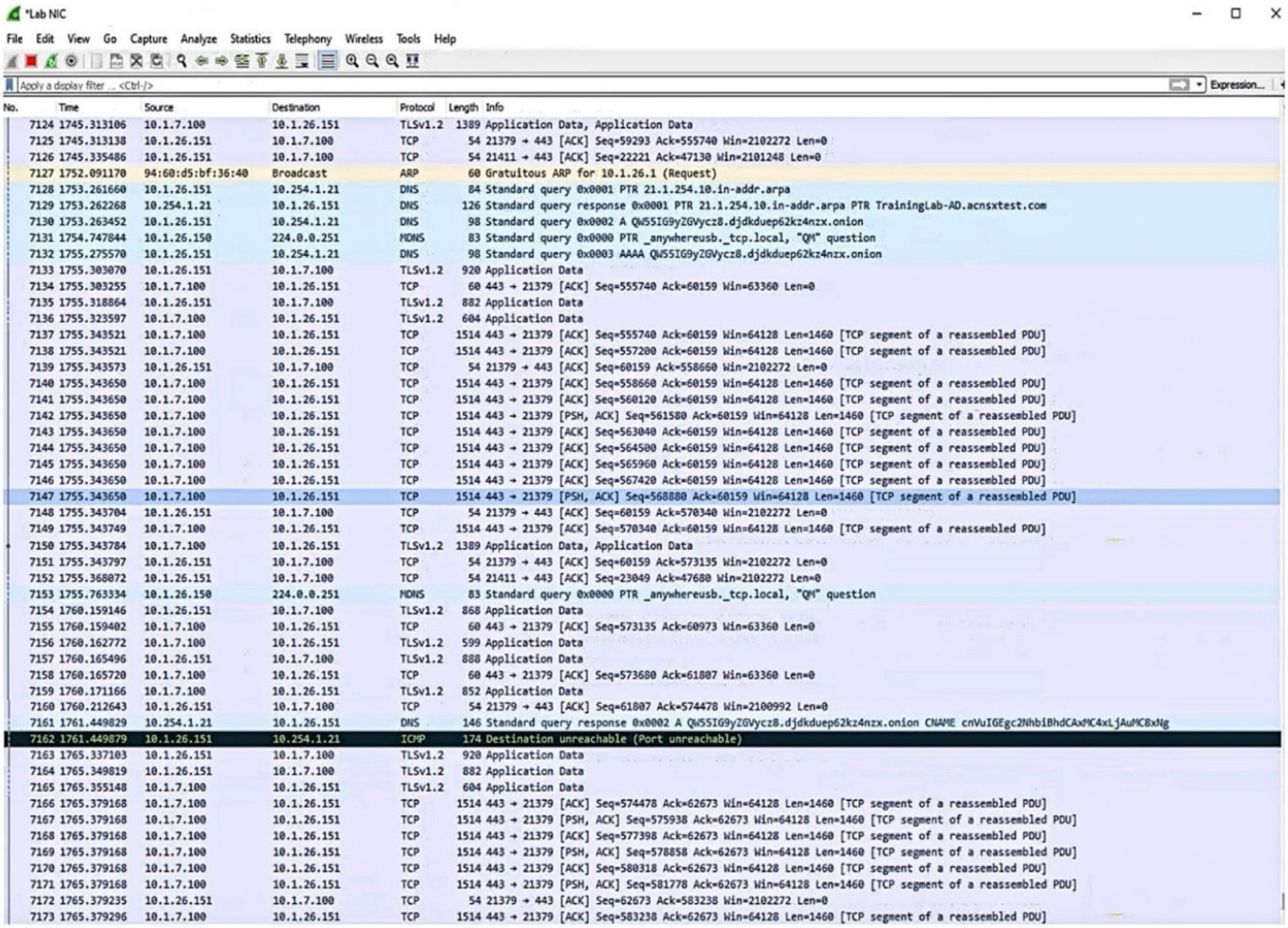
C. The ClearPass Onboard hostname referenced in Intune SCEP profiles

D. The hostname used by the on-prem domain controllers

Correct Answer: B

QUESTION 2

Refer to the exhibit.



Which security issue is possibly indicated by this traffic capture?

A. An attempt at a DoS attack by a device acting as an unauthorized DNS server

B. A port scan being run on the 10.1.7.0/24 subnet

C. A command and control channel established with DNS tunneling

D. An ARP poisoning or man-in-the-middle attempt by the device at 94:60:d5:bf:36:40

Correct Answer: C

DNS tunneling is a technique that abuses the DNS protocol to tunnel data or commands between a compromised host and an attacker\\'s server. DNS tunneling can be used to establish a command and control channel, which allows the attacker to remotely control the malware or exfiltrate data from the infected host1 The traffic capture in the exhibit shows some signs of DNS tunneling. The source IP address is 10.1.7.2, which is likely an internal host behind a firewall. The destination IP address is 8.8.8.8, which is a public DNS resolver. The DNS queries are for subdomains of badsite.com, which is likely a malicious domain registered by the attacker. The subdomains have long and random names, such as 0x2a0x2a0x2a0x2a0x2a0x2a0x2a0x2a.badsite.com, which could be used to encode data or commands. The DNS responses have large sizes, such as 512 bytes, which could be used to carry data or commands back to the host2

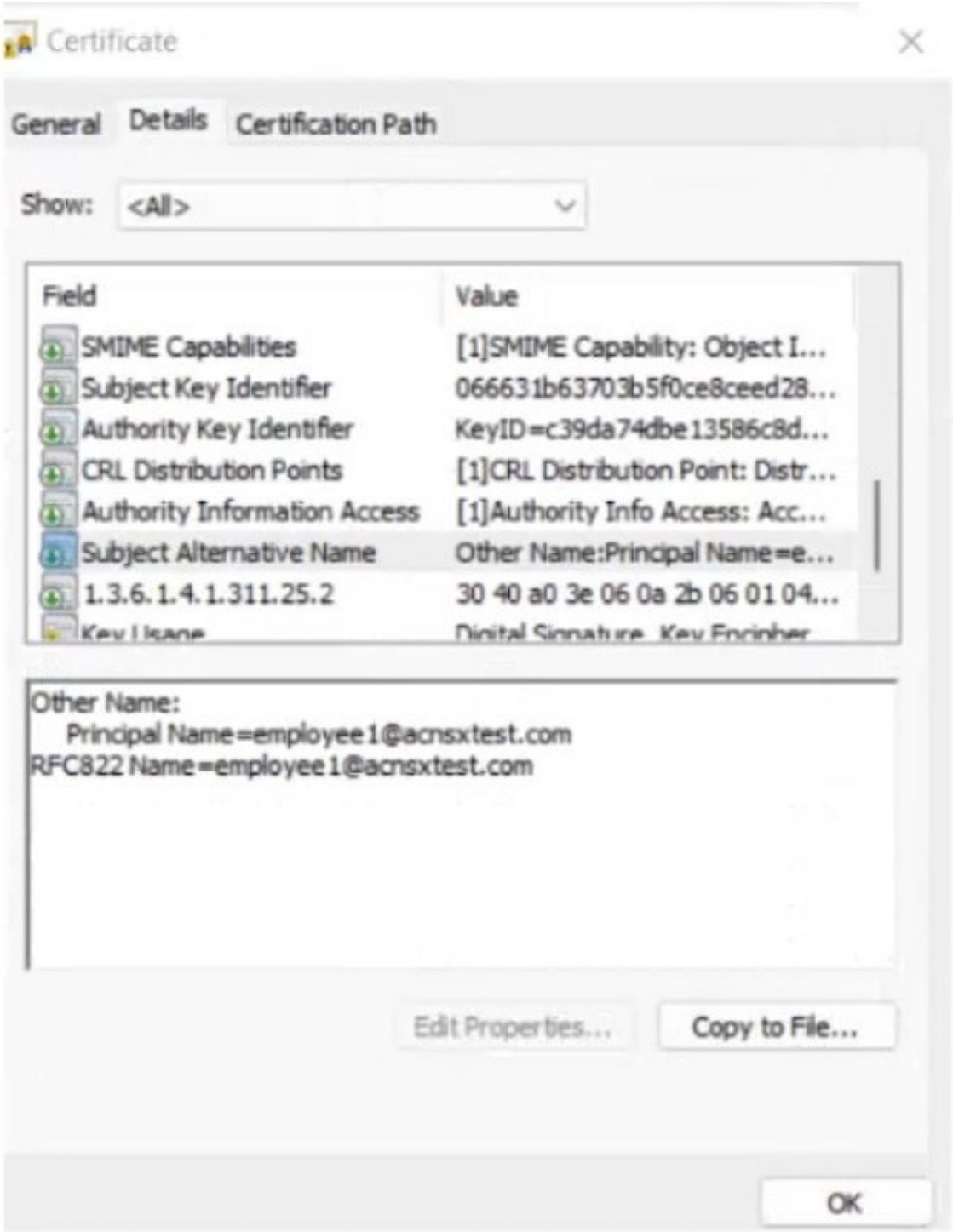
QUESTION 3

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.



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

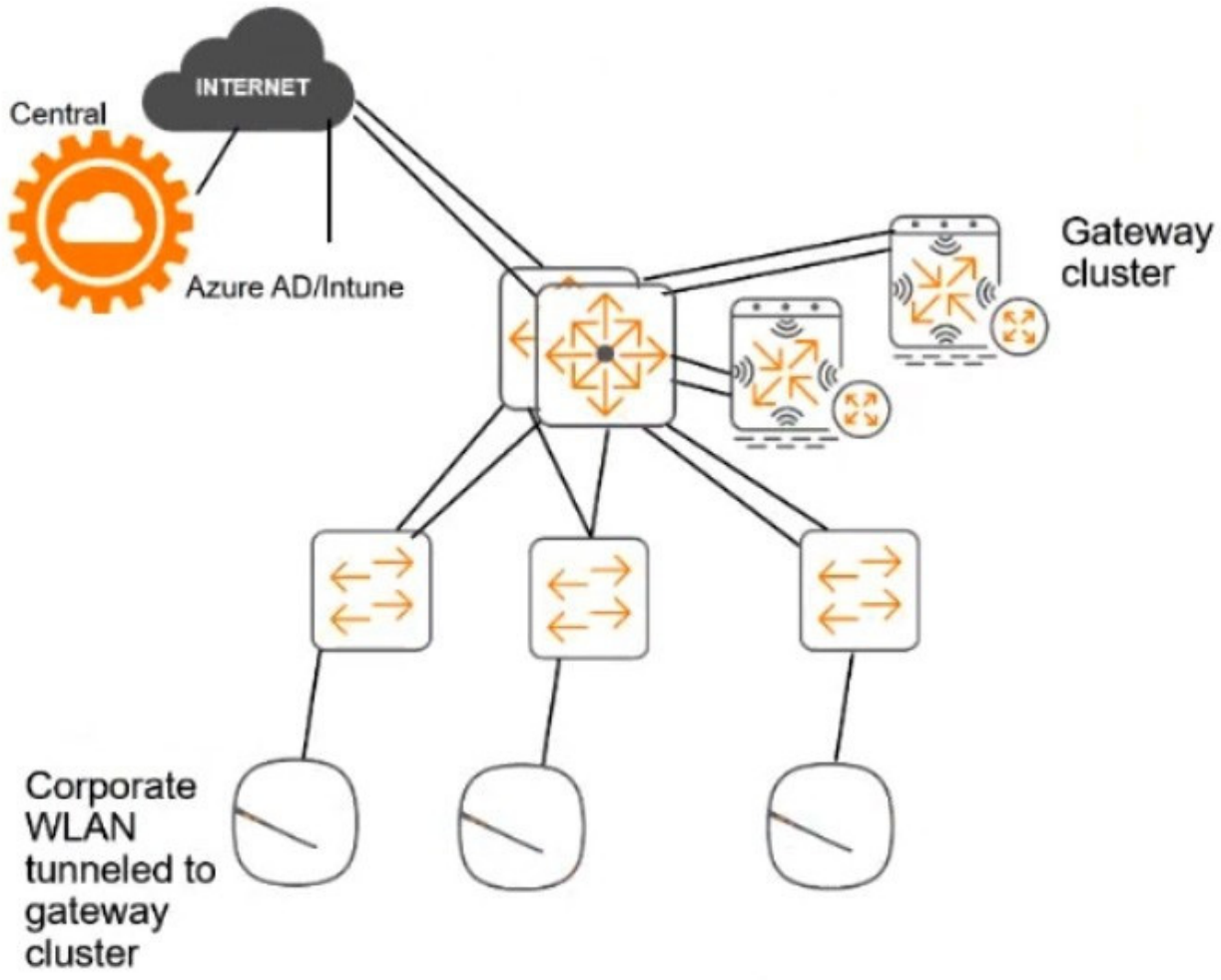
5.

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

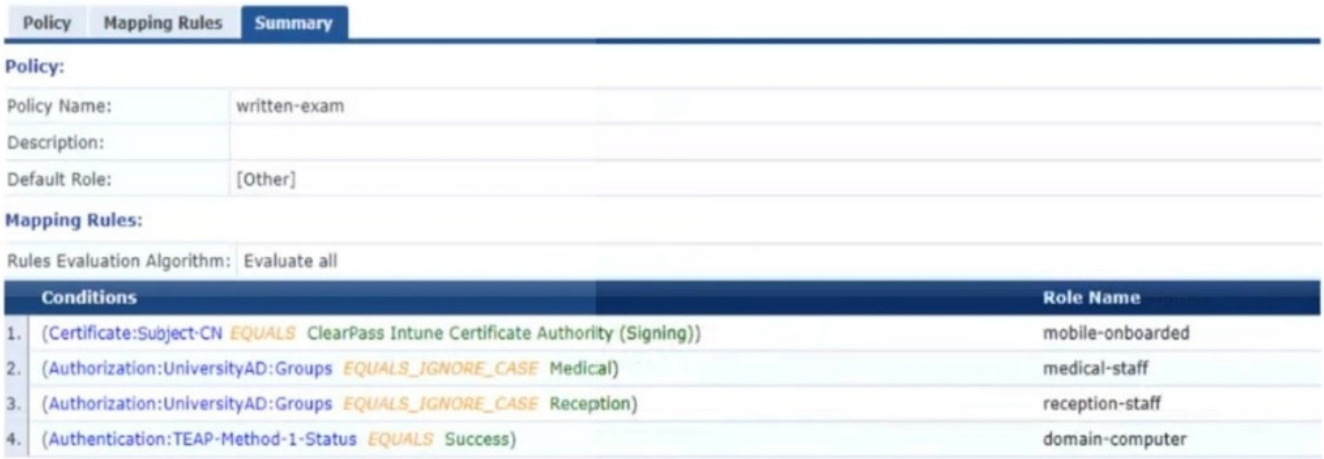
4.

radius.acnsxtest.com = 10.47.47.8

5.

onboard.acnsxtest.com = 10.47.47.8

You have created a role mapping policy as shown in the exhibits below.



What is one change that you need to make to this policy?

A. In rule 1 change Subject-CN to Issuer-CN.

B. Move rules 2 and 3 to the top of the list.

C. Change the rules evaluation mechanism to first applicable.

D. Change the default role to \\'mobile-onboarded*

Correct Answer: A

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.

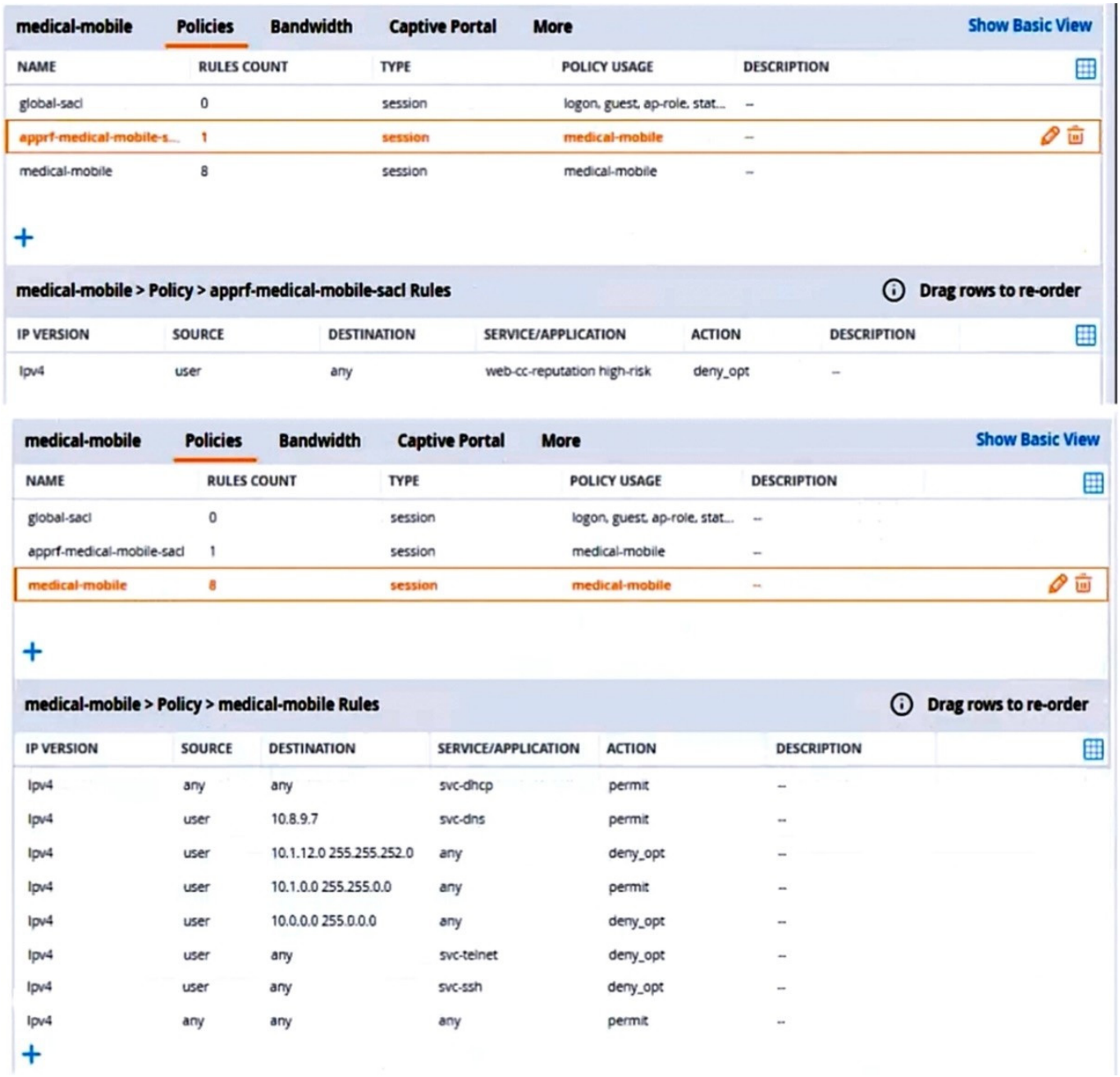
Denied access to the WLAN for a period of time if they send any Telnet traffic

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 exhibits below show the configuration for the role.



There are multiple issues with the configuration.

What is one of the changes that you must make to the policies 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, change the source in rule 1 to "user."

B. In the "medical-mobile" policy, change the subnet mask in rule 3 to 255.255.248.0.

C. In the "medical-mobile" policy, move rules 6 and 7 to the top of the list.

D. Move the rule in the "apprf-medical-mobile-sacl" policy between rules 7 and 8 in the "medical-mobile" policy.

Correct Answer: C

Rules 6 and 7 in the "medical-mobile" policy are used to deny access to the WLAN for a period of time if the clients send any SSH or Telnet traffic, as required by the scenario. However, these rules are currently placed below rule 5, which permits access to the Internet for any traffic. This means that rule 5 will override rules 6 and 7, and the clients will not be denied access to the WLAN even if they send SSH or Telnet traffic. To fix this issue, rules 6 and 7 should be moved to the top of the list, before rule 5. This way, rules 6 and 7 will take precedence over rule 5, and the clients will be denied access to the WLAN if they send SSH or Telnet traffic, as expected.

QUESTION 5

Refer to the scenario.

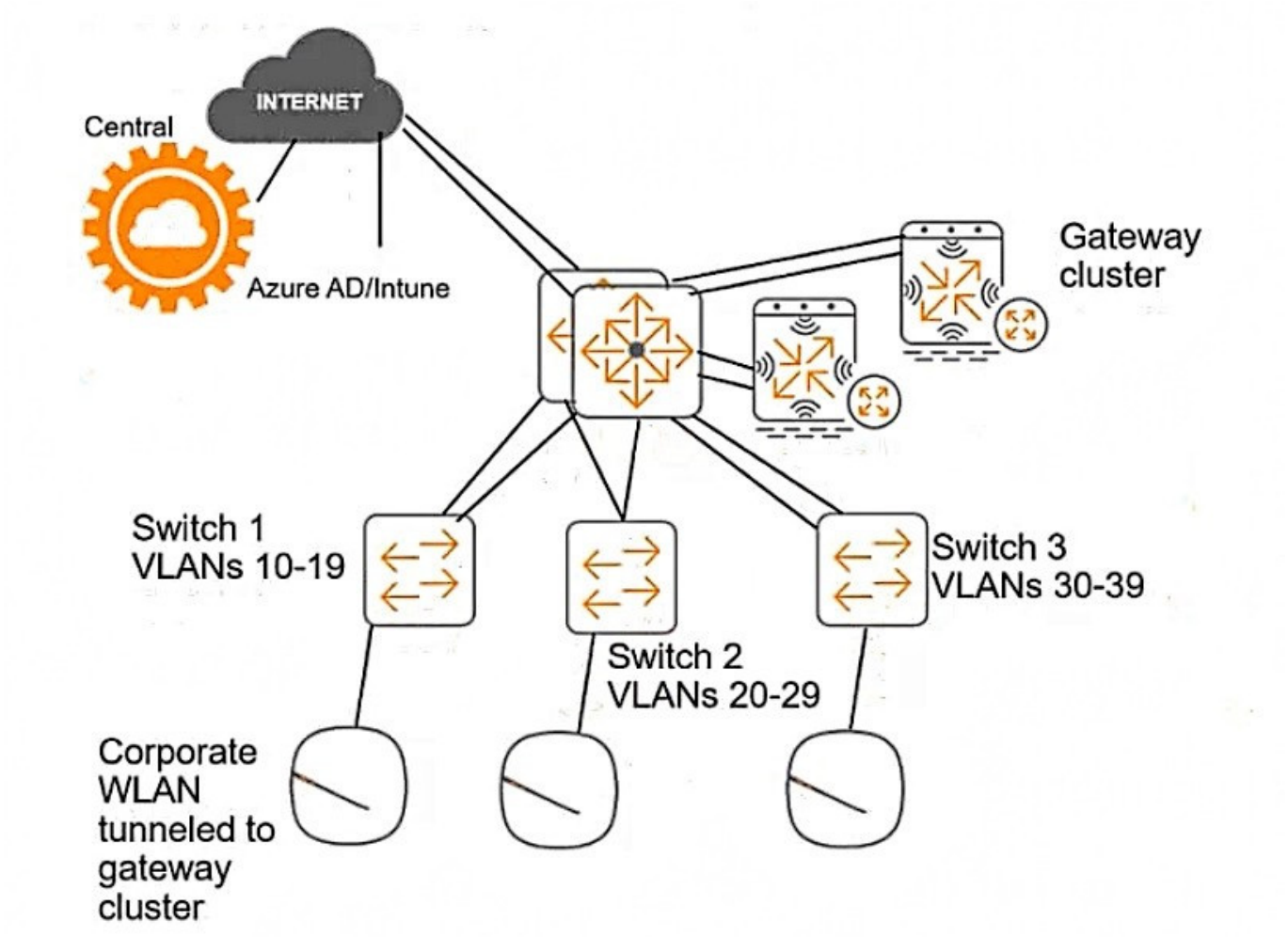
This customer is enforcing 802.1X on AOS-CX switches to Aruba ClearPass Policy Manager (CPPM). The customer wants switches to download role settings from CPPM. The "reception-domain" role must have these settings:

-- Assigns clients to VLAN 14 on switch 1, VLAN 24 on switch 2, and so on.

-- Filters client traffic as follows:

-- Clients are permitted full access to 10.1.5.0/24 and the Internet

-- Clients are denied access to 10.1.0.0/16 The switch topology is shown here:



How should you configure the VLAN setting for the reception role?

A. Assign a consistent name to VLAN 14, 24, or 34 on each access layer switch and reference that name in the enforcement profile VLAN settings.

B. Configure the enforcement profile as a downloadable role, but specify only the role name and leave the VLAN undefined. Then define a \\'reception\\' role with the correct VLAN setting on each individual access layer switch.

C. Assign a number-based ID to the access layer switches. Then use this variable in the enforcement profile VLAN settings: %(NAS-ID]4.

D. Create a separate enforcement profile with a different VLAN ID for each switch. Add all profiles to the profile list in the appropriate enforcement policy rule.

Correct Answer: A

According to the AOS-CX User Guide, one way to configure the VLAN setting for the reception role is to assign a consistent name to VLAN 14, 24, or 34 on each access layer switch and reference that name in the enforcement profile VLAN settings. This way, the switches can download the role settings from CPPM and apply the correct VLAN based on the name, rather than the ID. For example, the enforcement profile VLAN settings could be:

```
vlan-name reception-vlan
```

And the VLAN configuration on each switch could be:

```
vlan 14
name reception-vlan
exit
```

```
vlan 24
name reception-vlan
exit
```

```
vlan 34
name reception-vlan
exit
```

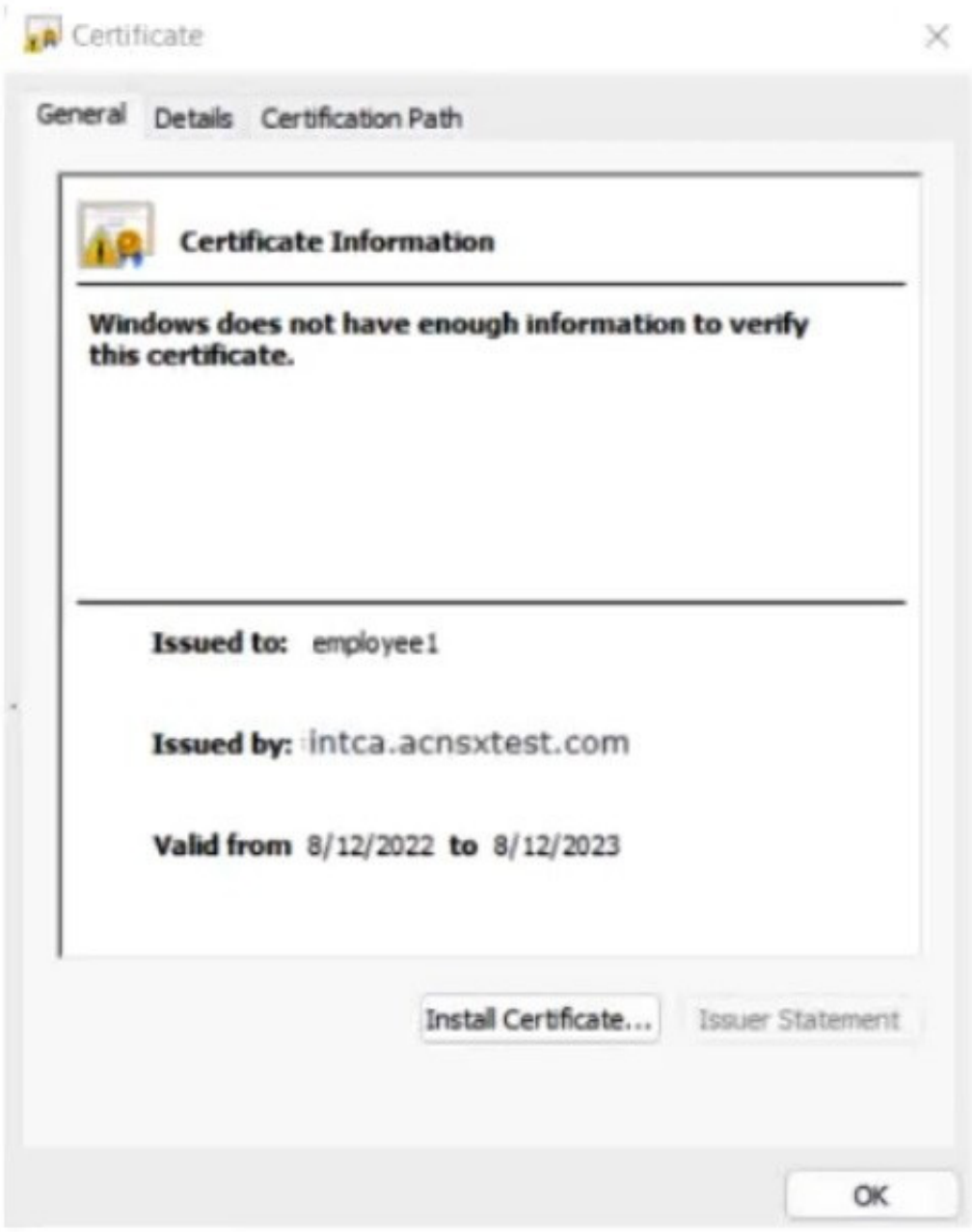
QUESTION 6

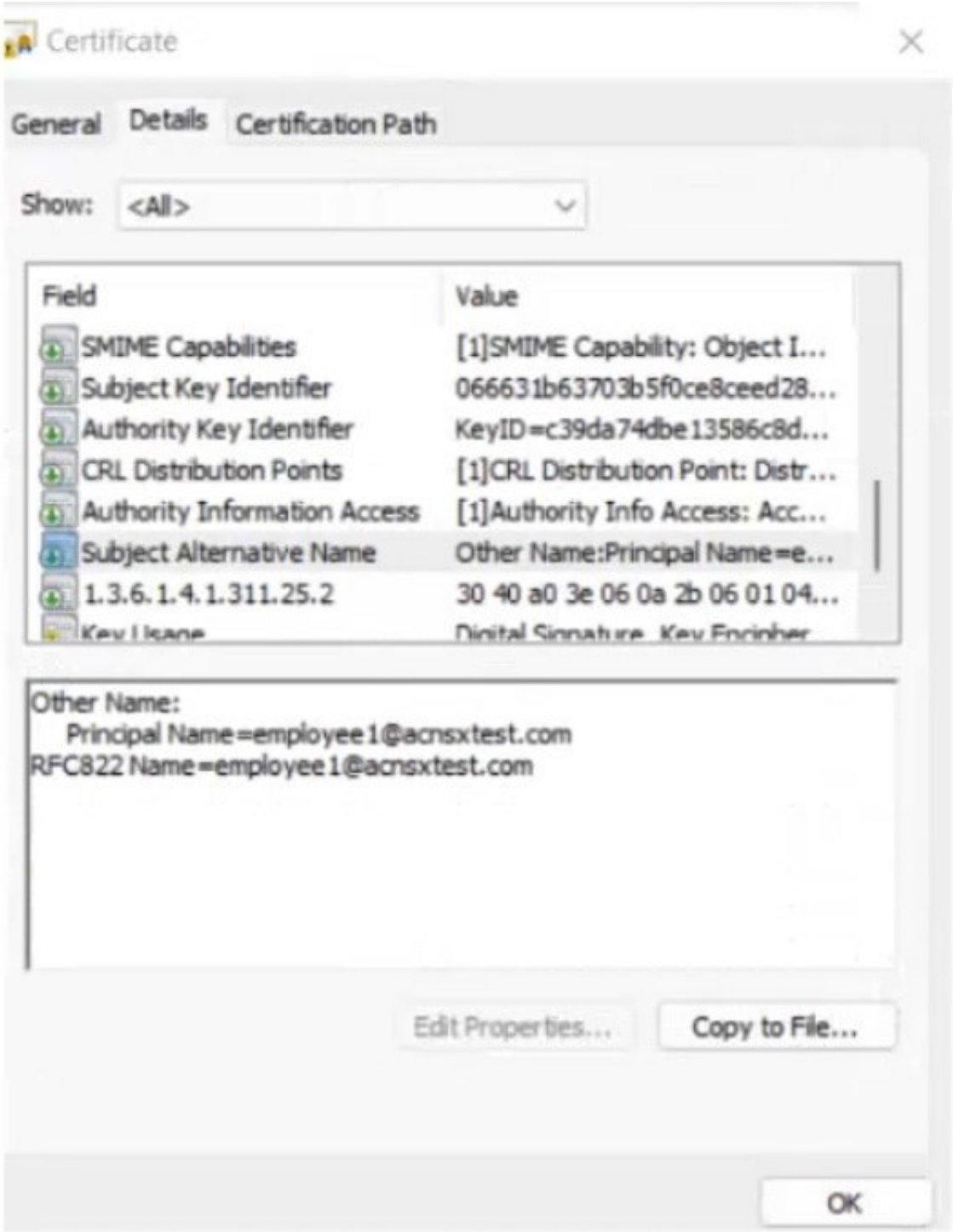
Refer to the scenario.

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.





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

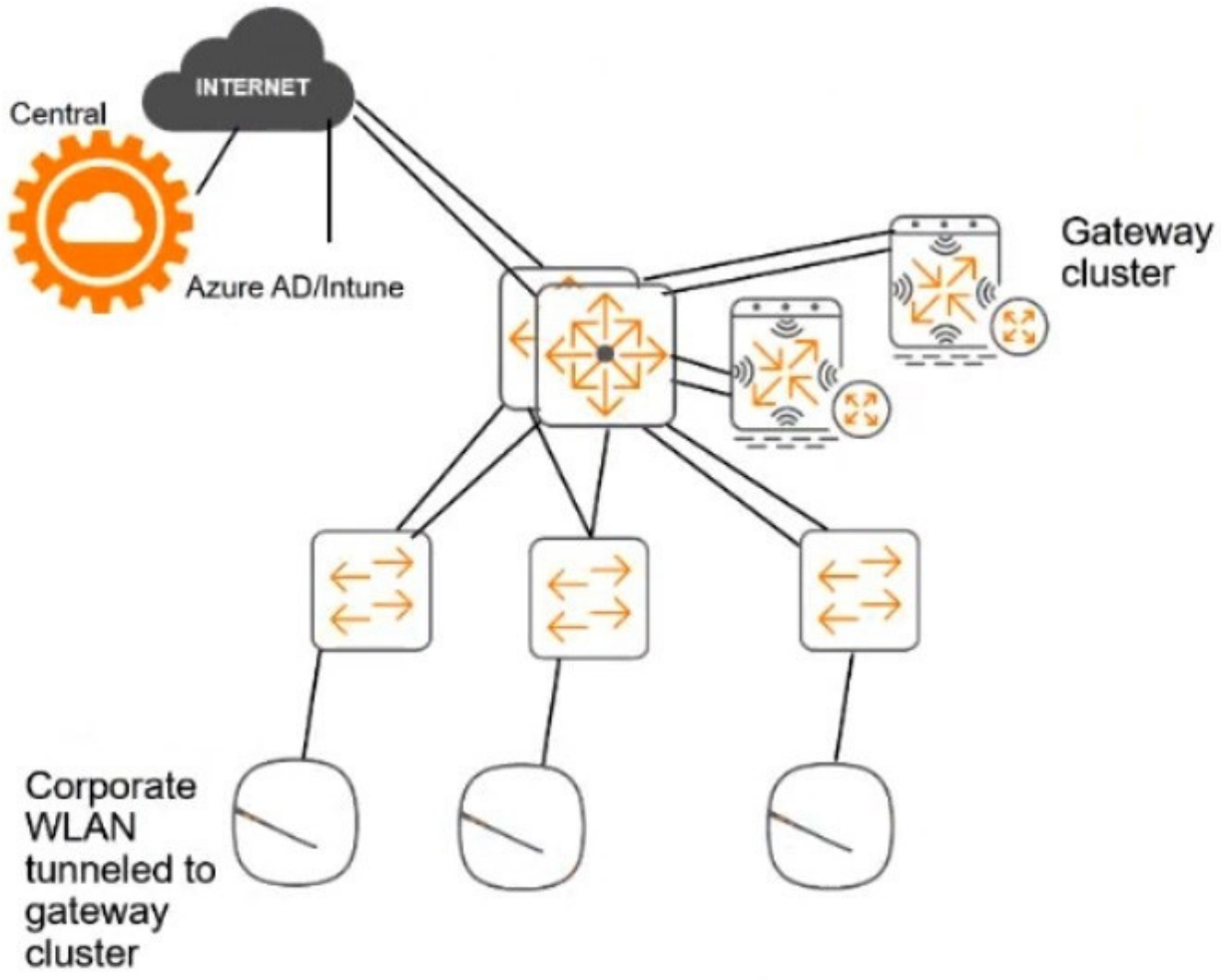
5.

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

You have imported the root certificate for the Windows CA to the ClearPass CA Trust list.

Which usages should you add to it based on the scenario requirements?

A. EAP and AD/LDAP Server

B. LDAP and Aruba infrastructure

C. Radsec and Aruba infrastructure

D. EAP and Radsec

Correct Answer: A

QUESTION 7

Refer to the scenario.

A customer is migrating from on-prem AD to Azure AD as its sole domain solution. The customer also manages both wired and wireless devices with Microsoft Endpoint Manager (Intune).

The customer wants to improve security for the network edge. You are helping the customer design a ClearPass deployment for this purpose. Aruba network devices will authenticate wireless and wired clients to an Aruba ClearPass Policy Manager (CPPM) cluster (which uses version 6.10).

The customer has several requirements for authentication. The clients should only pass EAP-TLS authentication if a query to Azure AD shows that they have accounts in Azure AD. To further refine the clients\\' privileges, ClearPass also should use information collected by Intune to make access control decisions.

Assume that the Azure AD deployment has the proper prerequisites established.

You are planning the CPPM authentication source that you will reference as the authentication source in 802.1X services.

How should you set up this authentication source?

A. As Kerberos type

B. As Active Directory type

C. As HTTP type, referencing the Intune extension

D. AS HTTP type, referencing Azure AD\\'s FODN

Correct Answer: D

An authentication source is a configuration element in CPPM that defines how to connect to an external identity provider and retrieve user or device information . CPPM supports various types of authentication sources, such as Active

Directory, LDAP, SQL, Kerberos, and HTTP .

To authenticate wireless and wired clients to Azure AD, you need to set up an authentication source as HTTP type, referencing Azure AD\\'s FQDN . This type of authentication source allows CPPM to use REST API calls to communicate with

Azure AD and validate the user or device credentials . You also need to configure the OAuth 2.0 settings for the authentication source, such as the client ID, client secret, token URL, and resource URL .

To use information collected by Intune to make access control decisions, you need to set up another authentication source as HTTP type, referencing the Intune extension . This type of authentication source allows CPPM to use REST API

calls to communicate with Intune and retrieve the device compliance status . You also need to configure the OAuth 2.0 settings for the authentication source, such as the client ID, client secret, token URL, and resource URL .

QUESTION 8

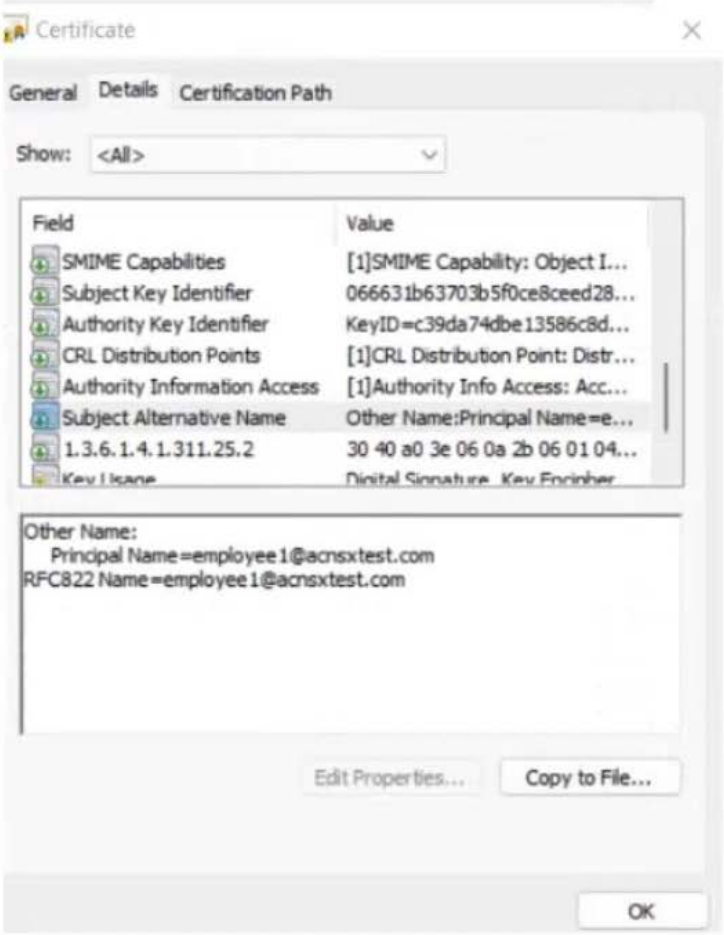
Refer to the scenario.

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
General
Details
Certification Path
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
Install Certificate...
Issuer Statement
OK


Certificate
General
Details
Certification Path
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...
Other Name:
Principal Name=employee1@acnsxtest.com
RFC822 Name=employee1@acnsxtest.com
Edit Properties...
Copy to File...
OK

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

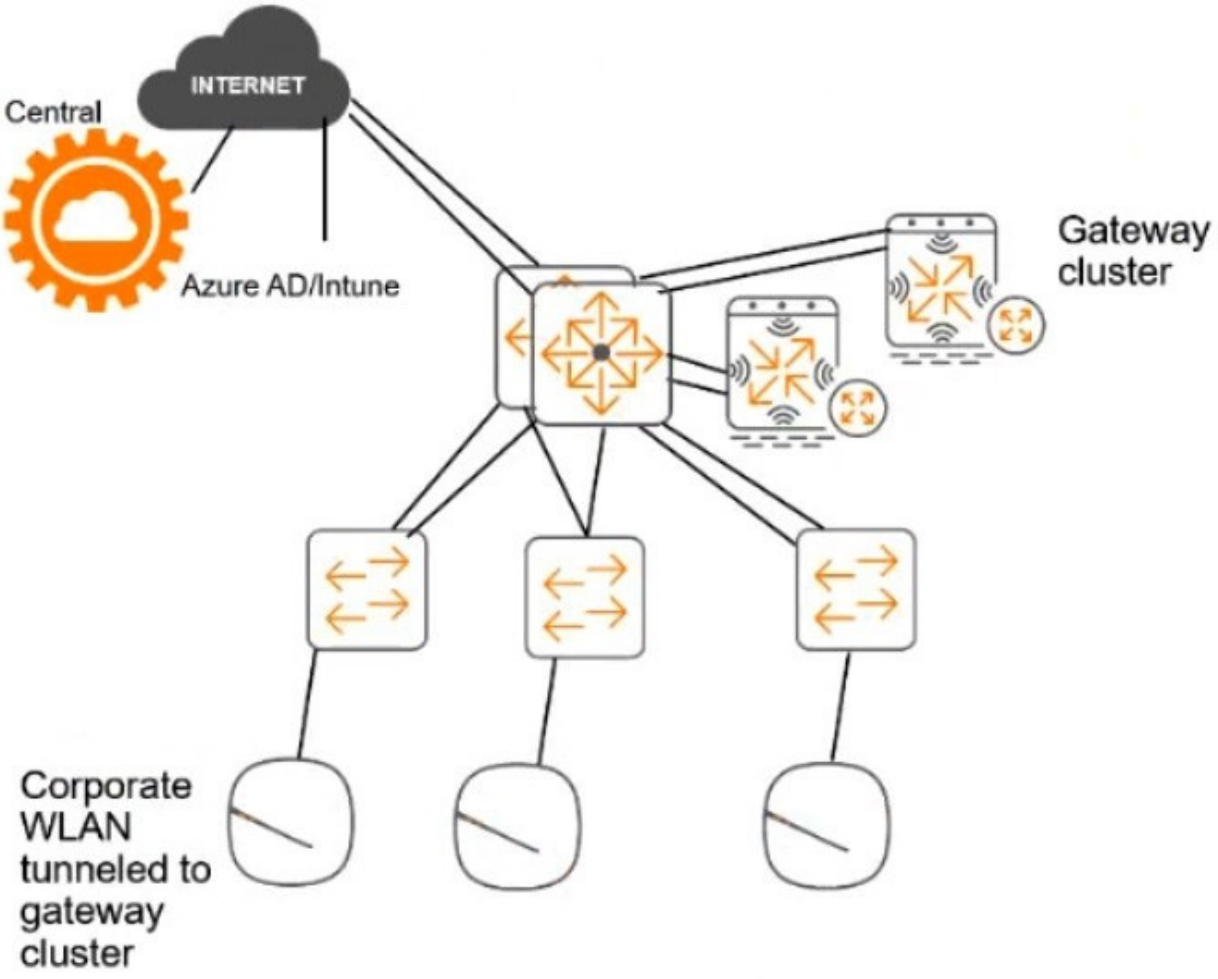
5.

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 You cannot see flow attributes for wireless clients. What should you check?

A. Deep packet inspection is enabled on the role to which the Aruba APs assign the wireless clients.

B. Firewall application visibility is enabled on the Aruba gateways, and the gateways have been rebooted.

C. Gateway IDS/IPS is enabled on the Aruba gateways, and the gateways have been rebooted.

D. Deep packet inspection is enabled on the Aruba Aps, and the APs have been rebooted.

Correct Answer: A

QUESTION 9

Refer to the scenario.

A customer has asked you to review their AOS-CX switches for potential vulnerabilities. The configuration for these switches is shown below:

```
hostname Access-Switch-$$

ntp authentication-key 1 sha1 ciphertext
AQBapYn45h7mDzxcLhAYWBH6biegegFASS1kvTQPPgICEfaLCAAAAMIb48QNRhSg
ntp trusted-key 1
ntp server pool.ntp.org minpoll 4 maxpoll 4 iburst key-id 1
ntp enable
ntp authentication
!
radius-server host rad.example.com tls
!
tacacs-server host rad.example.com
!
aaa authentication login ssh group tacacs local
aaa authentication login telnet group tacacs local
!
aaa accounting port-access start-stop interim group radius
!
radius dyn-authorization enable
!
radius dyn-authorization client rad.example.com tls
ssh server vrf default
ssh server vrf mgmt
telnet server vrf default
telnet server vrf mgmt
crypto pki application radsec-client certificate device-identity
crypto pki ta-profile privateca
ta-certificate
      -----BEGIN CERTIFICATE-----
      MIIGAzCCA+ugAwIBAgIUEVfsxopuixT2QHZDJ/UYAAbYsdowDQYJKoZIhvcNAQEL
      BQAwgYgxCzAJBgNVBAYTAlVTMRMwEQYDVQQIDApDYWxpZm9ybmlhMRIwEAYDVQQH
      DAlTdW5ueXZhbGUxHDAaBgNVBAoME0FydWJhIFRyYWluaW5nIExhYnMxEzARBgNV
      BAsMCkFDTlNYIFRlc3QxHTAbBgNVBAMMFHJvb3RjYS5hY25zeHRlc3QuY29tMB4X
      DTIyMTEyMjIwNTQxOFoXDTMyMTExOTIwNTQxOFowgYgxCzAJBgNVBAYTAlVTMRMw
      EQYDVQQIDApDYWxpZm9ybmlhMRIwEAYDVQQHDAlTdW5ueXZhbGUxHDAaBgNVBAoM
      E0FydWJhIFRyYWluaW5nIExhYnMxEzARBgNVBAsMCkFDTlNYIFRlc3QxHTAbBgNV
      BAMMFHJvb3RjYS5hY25zeHRlc3QuY29tMIICIjANBgkqhkiG9w0BAQEFAAOCAg8A
      MIICCgKCAgEAsiUzsBkJcUgcdsbRyoLd0ZNqpcXfphk2VsSzZngP1LCu3lea3OHU
      V9GchhJXOQaI3HDUTcLp4b5If63z4nKzA36T6tyWXOe0PSgUjy+61XXMA9Rp5DKc
      CyoY9F8spVJiEo2n2hqL4m/DLFYlhxo5Z2UKav/08DMfzD/yVUzGNiQKDP/L7ivk
      CWF+15WIGSrH10i/rgIM/+W20n58aDx5f1AWaH9DYdRTWFMuk1UXQ/I8+7+9PXju
      B95Mt4b77RaWWj6CkW9k8WhmyjE7MMPSHtuJ4t3evh7jd/lTkm5ZOg/V8kvNTtW5
      fif7lkWLevmlLlvcxYnj+S3CWhAFdaR7S33a6xwdZxCDOLfPB6L1oOnKe0VM4mO2
      lOZtJNPFueBt16BRolR+IMANQkj3B2lB0whSLHF6JmLr0L6y/edV8XhIUhMxOfIp
      JKeSw38TDm3t1k98PBCOaLj5s4tYJRxcZLDnrg7Oz1e37sxENYoBtgRp77cdfePr
      cP/sp8U66gti2F0ijkU6k37moL3sMs2uHgC0YWpfRyFI09BWCRbxmy81UePiSlsW
      0goOaPDr35W/0443I/z6A+q/ciwVrALS+zEfHbMDFxo4VMygJttaiWZ05GAQQSHj
      redQmQEQPMwkgbzaELtAgYOWGkB56T/XifRLVxneYU8woAEZwmscI3kCAwEAAaNj
      MGEwHQYDVR0OBBYEFGXCH/z475pdNKIHhjDxFCfjz8khMB8GA1UdIwQYMBaAFGXC
      H/z475pdNKIHhjDxFCfjz8khMA8GA1UdEwEB/wQFMAMBAf8wDgYDVR0PAQH/BAQD
      AgGGMA0GCSqGSIb3DQEBCwUAA4ICAQB5TGIspaamHQXtsnWgmux6PANdEdPZ0Ele
      wDnpUxkVbeSPr9wl8luRJMptRO25rwVwEtrM8t5JD4jAK+d0usr4TDKwWqPPqFi0
      F5svFK9aEJ59ceD+eDWl4LAJJi3zjb9ZBuBa3LkaP7kyTlSnI0+opN+vdV43LNXh
      T23xEmLC9OUolq3bb8zpkWXieeFwSo2BafFMscPdf75DVY+x+Qo1SgpjbWBAS80B
      jRdZHrKmsqcrIG+37bixqaFj9nMzWpX0n2HfKCVcl6uk2pDNbiYVbU3k9b/ZWQmW
      DRYkAuR8dFBN3lKDyQo86T/chT/DY77FoStfg0gDZEj3EqaM76rf8S2z1GCsrfkp
      Crp5oKP6jiOCi2EcidkZSsmbzAHWKXNaF7vWRj0OivpqEFRkIVu/kce9O2KaxNYd
      sIKlNh7gG4pcQqhFfDddFD9vXvjOwKnXKkKppUpN6w+Quc+jhqFpP8GVPOy7ayZo
      z5cz5yEaVXtbfXRhVSg9oooq7xImBT14SK1pyrHSj8sD67Og3zgnNot/v8fHhI3O
      zUtBe4UPGWfraO4gkHH3mbb1qYeJnxKpMz56A0APBkKV9icY0uTQOsHk6bA9lG+Q
      sjqyWwKApf7RB4lHjF+7FfMU6UJnZBm75zQ89CPAPCoVeJ6fNNr/aO+3VrNz4j9l
      Nr63M6xeYw==
      -----END CERTIFICATE-----
        END_OF_CERTIFICATE
  vsf member 1
    type jl666a
  dhcpv4-snooping
  vlan 1
  vlan 2
  vlan 4
    dhcpv4-snooping
  spanning-tree
  interface mgmt
    no shutdown
  aaa authentication port-access dot1x authenticator
    enable
  interface lag 1
    no shutdown
    no routing
    vlan trunk native 1
    vlan trunk allowed 2,4
    dhcpv4-snooping trust
  interface 1/1/1-1/1/24
    no shutdown
    no routing
    vlan access 4
    aaa authentication port-access dot1x authenticator
      enable
  interface vlan 1
  interface vlan 2
    ip address 10.1.2.1/24
  ip route 0.0.0.0/0 10.1.2.254
  ip dns domain-name example.com
  ip dns server-address 10.1.1.9
  !
  https-server vrf default
  https-server vrf mgmt
```

What is one recommendation to make?

A. Let the RADIUS server confiqure VLANs on LAG 1 dynamically.

B. Use MDS instead of SHA1 for the NTP authentication key.

C. Encrypt the certificate in the TA-profile.

D. Create a control plane ACL to limit the sources that can access the switch with SSH.

Correct Answer: D

According to the AOS-CX Switches Multiple Vulnerabilities1, one of the vulnerabilities (CVE-2021-41000) affects the SSH service on AOS-CX switches. This vulnerability allows an unauthenticated remote attacker to cause a denial-of-service condition on the switch by sending specially crafted SSH packets. The impact of this vulnerability is high, as it could result in a loss of management access and network disruption. Therefore, one recommendation to make is to create a control plane ACL to limit the sources that can access the switch with SSH. This way, the switch can filter out unwanted or malicious SSH traffic and reduce the risk of exploitation.

QUESTION 10

A customer requires a secure solution for connecting remote users to the corporate main site. You are designing a client-to-site virtual private network (VPN) based on Aruba VIA and Aruba Mobility Controllers acting as VPN Concentrators (VPNCs). Remote users will first use the VIA client to contact the VPNCs and obtain connection settings.

The users should only be allowed to receive the settings if they are the customer\\'s "RemoteEmployees" AD group. After receiving the settings, the VIA clients will automatically establish VPN connections, authenticating to CPPM with certificates.

What should you do to help ensure that only authorized users obtain VIA connection settings?

A. Set up the VPNCs\\' VIA web authentication profile to use CPPM as the authentication server; set up a service on CPPM that uses AD as the authentication source.

B. Set up the VPNCs\\' VIA web authentication profile to use an AD domain controller as the LDAP server.

C. Set up the VPNCs\\' VIA connection profile to use two authentication profiles, one RADIUS profile to CPPM and one LDAP profile to AD.

D. Set up the VPNCs\\' VIA connection profile to use one authentication profile, which is set to the AD domain controller\\'s hostname.

Correct Answer: A

The VIA web authentication profile is used to authenticate the users who want to download the VIA connection settings from the VPNCs. The VPNCs can use either an internal database or an external server (such as RADIUS or LDAP) as the authentication source for this profile. To ensure that only authorized users obtain VIA connection settings, you should use CPPM as the external server and configure a service on CPPM that uses AD as the authentication source. This way, you can leverage the role mapping and enforcement features of CPPM to check if the users belong to the "RemoteEmployees" AD group and grant or deny them access accordingly The other options are not correct because they do not allow you to verify the users\\' AD group membership before providing them with VIA connection settings. Option B would only check the users\\' credentials against AD, but not their group membership. Option C would only apply to the VPN connection phase, not the VIA connection settings phase. Option D would not work because the VPNCs do not support LDAP as an authentication source for VIA connection profiles

Reference:

1: Configuring the VIA Controller - Aruba, section "Configuring VIA Web Authentication Profile"

2: Configuring VIA Connection Profile - Aruba, section "Configuring Authentication Profile"

QUESTION 11

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 12

Refer to the scenario.

A customer is using an AOS 10 architecture with Aruba APs and Aruba gateways (two per site). Admins have implemented auto-site clustering for gateways with the default gateway mode disabled. WLANs use tunneled mode to the

gateways.

The WLAN security is WPA3-Enterprise with authentication to an Aruba ClearPass Policy Manager (CPPM) cluster VIP. RADIUS communications use RADIUS, not RadSec.

For which devices does CPPM require network device entries?

A. Forgateways\\' actual IP addresses and dynamic authorization VRRP addresses

B. For gateways\\' actual IP addresses and AP clusters\\' virtual IP addresses for dynamic authorization

C. For APs\\' actual IP addresses

D. ForAP clusters\\'virtual IP addresses

Correct Answer: A

ClearPass Policy Manager (CPPM) requires network device entries for the devices that communicate with it using RADIUS or TACACS+ protocols. In this scenario, the gateways are the devices that act as RADIUS clients and send authentication requests to CPPM for the WLAN users. Therefore, CPPM needs to have network device entries for the gateways\\' actual IP addresses and the shared secrets that match the ones configured on the gateways.

Additionally, CPPM also requires network device entries for the gateways\\' dynamic authorization VRRP addresses, which are used for sending CoA messages to the gateways. CoA messages are used to change the attributes or status of a user session on the gateways without requiring re-authentication. For example, CPPM can use CoA to apply policies, roles, or bandwidth limits based on various conditions. To enable VRRP IP addresses for dynamic authorization, you need to set up gateway clusters manually and assign a VRRP VLAN and a VRRP IP address to each cluster. This way, CPPM can use the VRRP IP address as the NAS IP address for RADIUS communications and CoA messages. The VRRP IP address will remain the same even if the active gateway in the cluster changes due to a failover event, ensuring seamless operations.