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

Aruba Certified Network Security Expert Written

Pass HP HPE6-A84 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/hpe6-a84.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by HP Official Exam Center

QUESTION 1

Refer to the scenario.

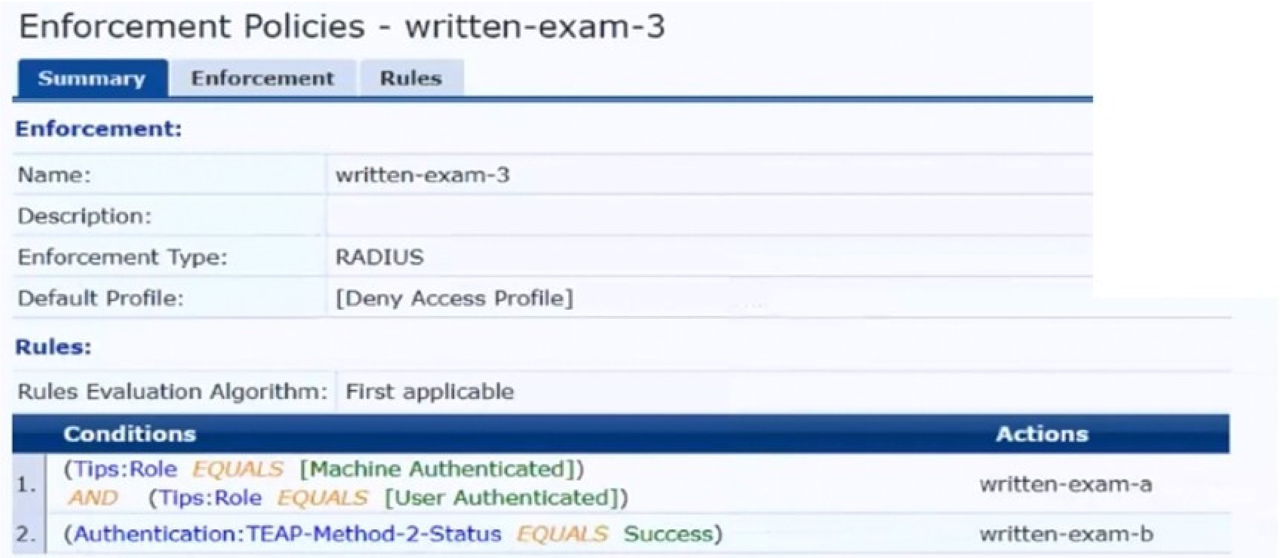
A customer has an Aruba ClearPass cluster. The customer has AOS-CX switches that implement 802.1X authentication to ClearPass Policy Manager (CPPM).

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

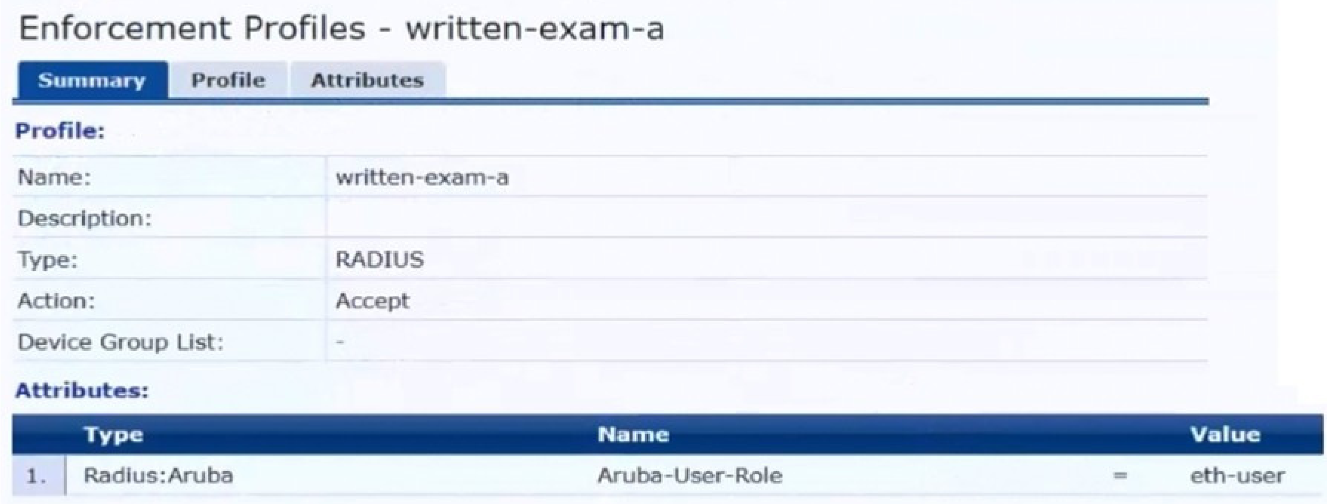
Enforcement:

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



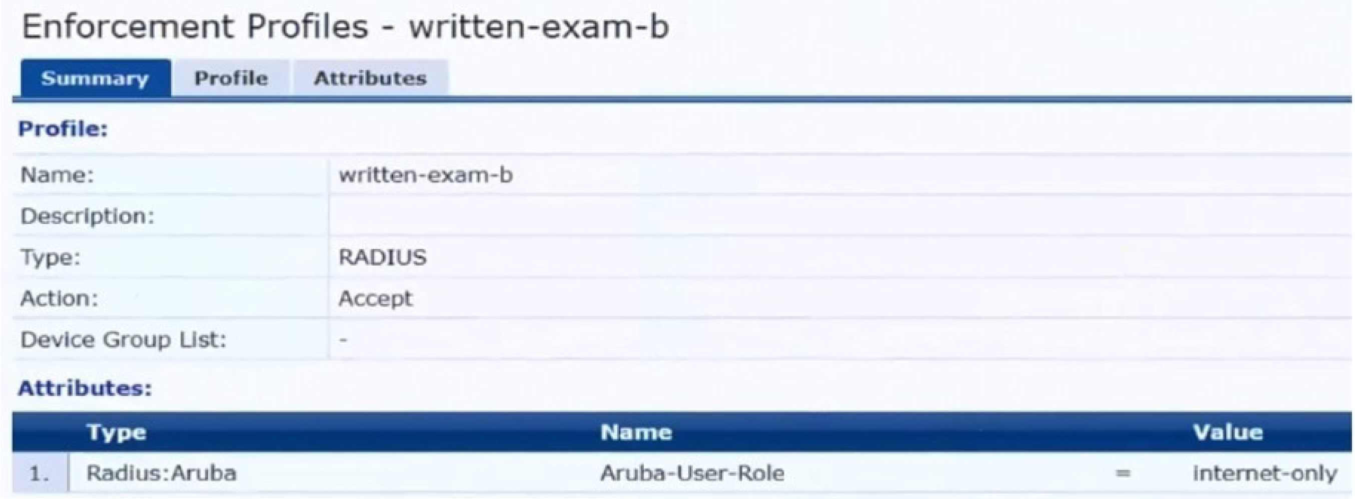
Enforcement Profiles - written-exam-a

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

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

1.

VLAN 4085 (system IP) = 10.20.4.21

2.

VLAN 20 (users) = 10.20.20.1

3.

VLAN 4094 (WAN) = 198.51.100.14

Gateway 2

1.

VLAN 4085 (system IP) = 10.20.4.22

2.

VLAN 20 (users) = 10.20.20.2

3.

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 are using the "myzone" name for the UBT zone.

Which is a valid minimal configuration for the AOS-CX port-access roles?

A. port-access role eth-internet gateway-zone zone myzone gateway-role eth-user

B. port-access role internet-only gateway-zone zone myzone gateway-role eth-internet

C. port-access role eth-internet gateway-zone zone myzone gateway-role eth-internet vlan access 20

D. port-access role internet-only gateway-zone zone myzone gateway-role eth-internet vlan access 20

Correct Answer: B

The UBT solution requires that the edge ports on the switches are configured in VLAN trunk mode, not access mode. This is because the UBT solution uses a special VLAN (VLAN 4095 by default) to encapsulate the user traffic and tunnel it to the gateway. The edge ports need to allow this VLAN as well as any other VLANs that are used for management or control traffic. Therefore, the edge ports should be configured as VLAN trunk ports and allow the necessary VLANs

QUESTION 2

A customer has an AOS 10 architecture, consisting of Aruba AP and AOS-CX switches, managed by Aruba Central. The customer wants to obtain information about the clients, such as their general category and OS. What should you explain?

A. The customer must deploy Aruba gateways in order to receive any client profiling information.

B. You will need to set up Aruba Central as a secondary IP helper for client VLANs, but this will not interfere with existing operations.

C. Aruba Central will automatically derive this information using telemetry from the Aruba devices.

D. The customer should set up a dedicated switch VSX group to sniff packets and direct them to Aruba Central.

Correct Answer: C

Aruba Central can provide visibility and profiling of clients using the Client Insights feature, which is an AI-powered solution that uses native infrastructure telemetry to identify and classify clients based on their OS and general category. This feature does not require any additional hardware or software, such as gateways, IP helpers, or packet sniffers. It works by collecting and analyzing data from the Aruba APs and AOS-CX switches that are managed by Aruba Central. You can find more information about Client Insights in the Visibility and profiling solutions | HPE Aruba Networking page and the Clients Profile - Aruba page.

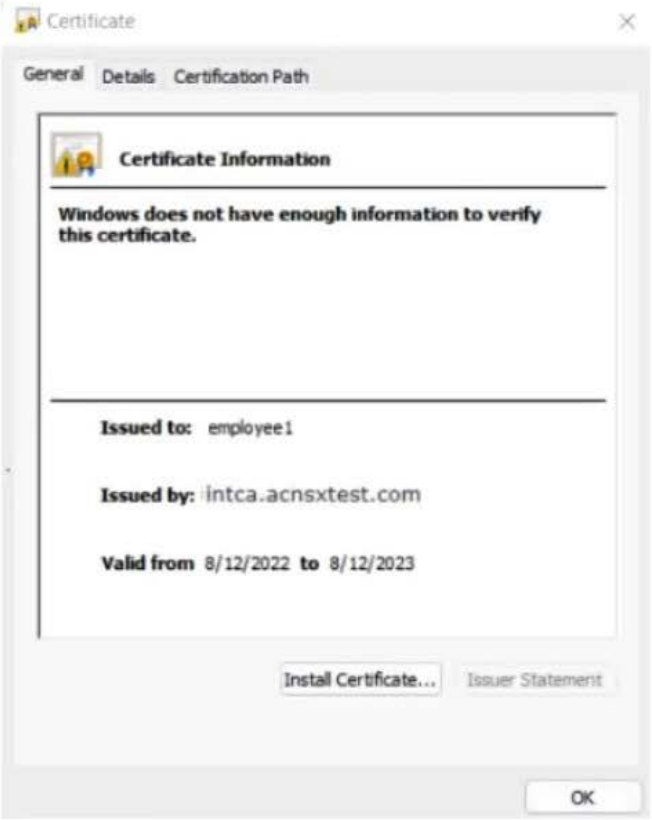
QUESTION 3

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.

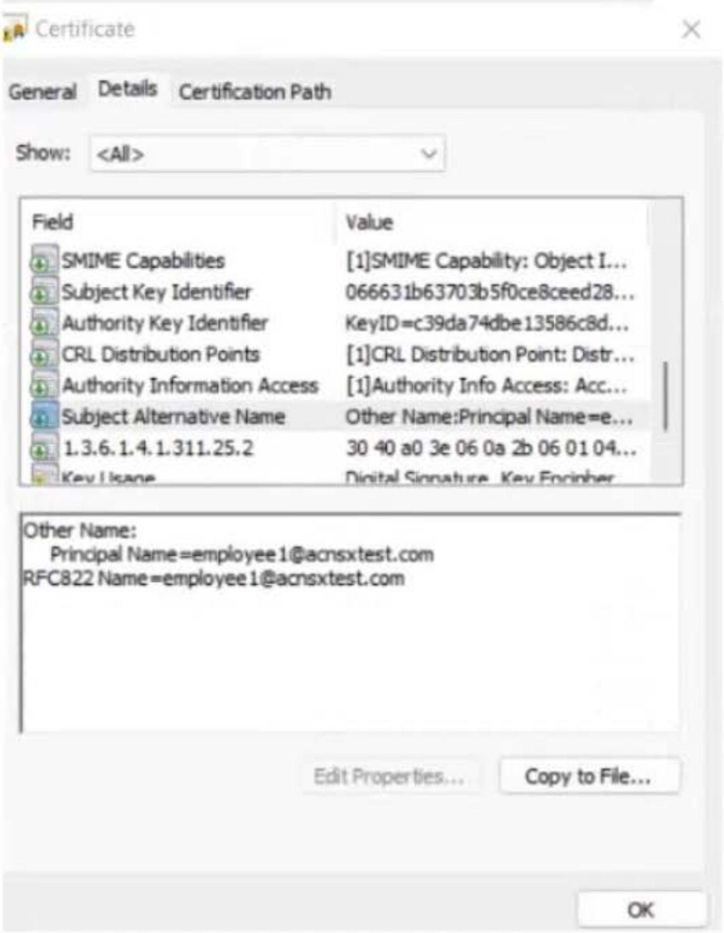


Windows does not have enough information to verify this certificate.

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

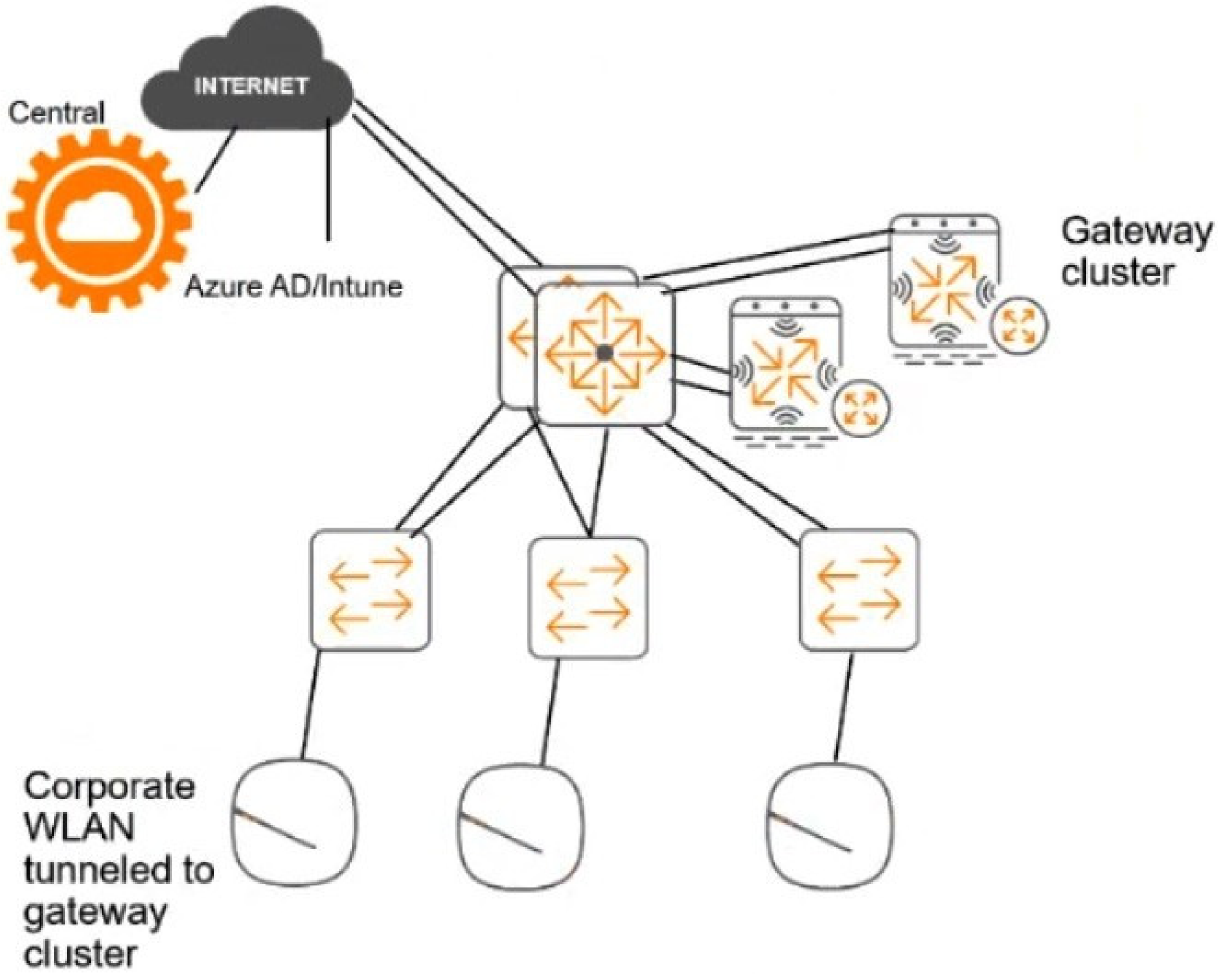
5.

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 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 4

Refer to the scenario.

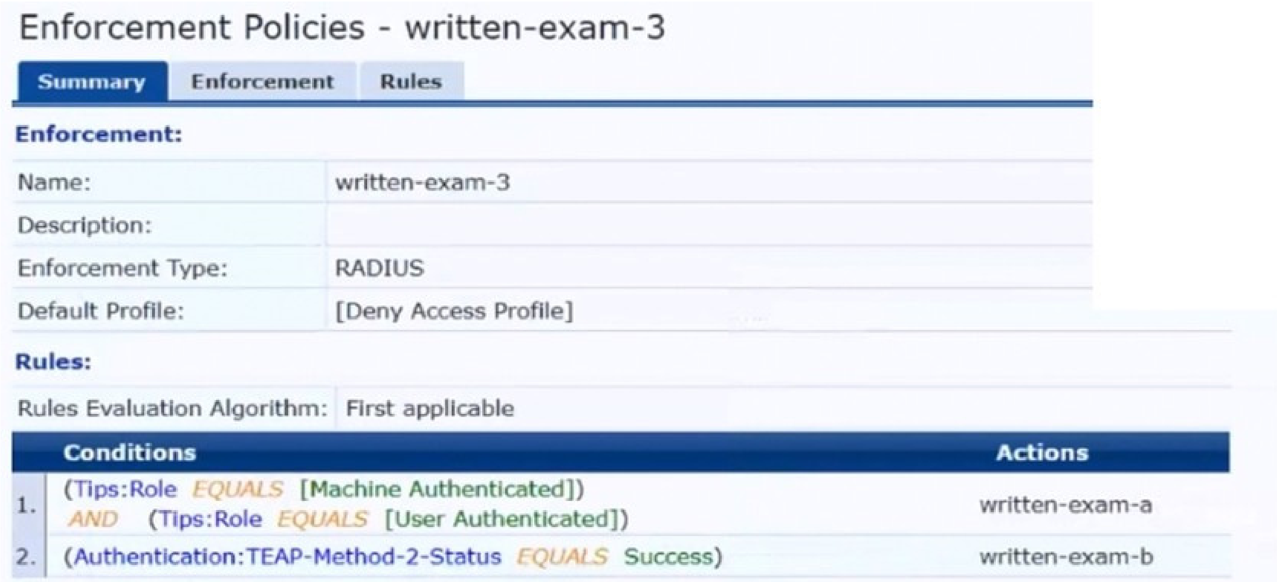
A customer has an Aruba ClearPass cluster. The customer has AOS-CX switches that implement 802.1X authentication to ClearPass Policy Manager (CPPM).

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

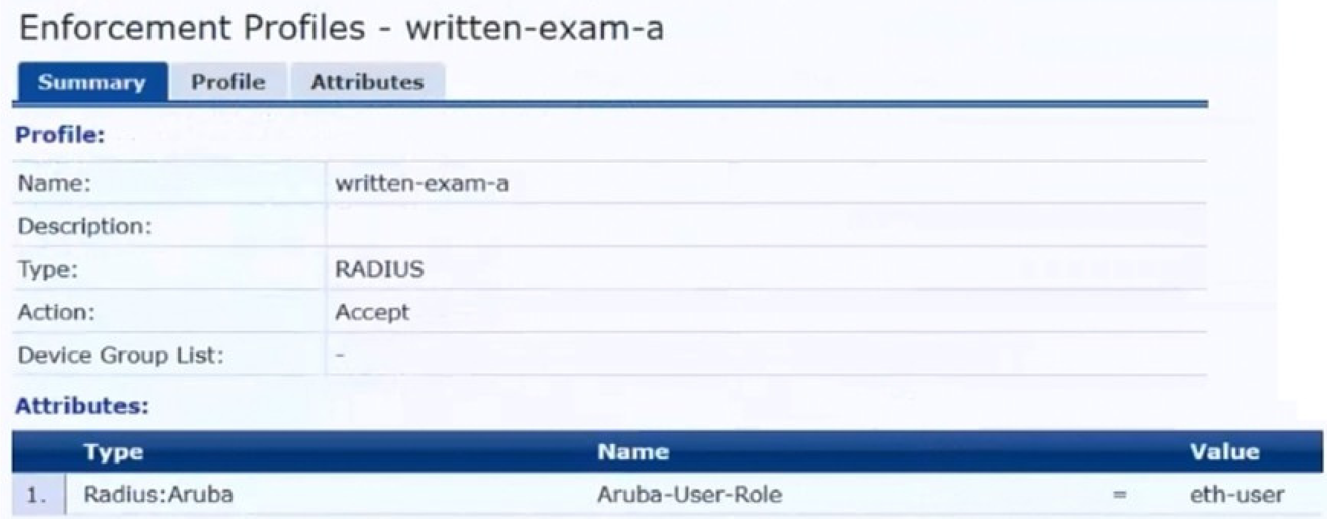
Enforcement:

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



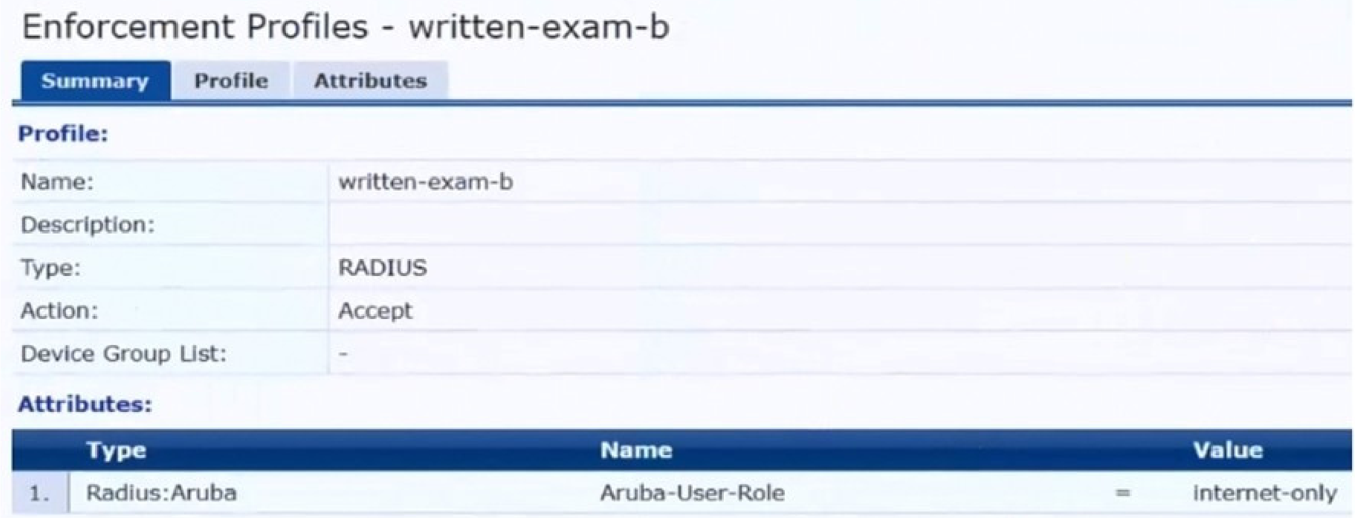
Enforcement Profiles - written-exam-a

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

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

1.

VLAN 4085 (system IP) = 10.20.4.21

2.

VLAN 20 (users) = 10.20.20.1

3.

VLAN 4094 (WAN) = 198.51.100.14

Gateway 2

1.

VLAN 4085 (system IP) = 10.20.4.22

2.

VLAN 20 (users) = 10.20.20.2

3.

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.

What is one change that you should make to the solution?

A. Change the ubt-client-vlan to VLAN 13.

B. Configure edge ports in VLAN trunk mode.

C. Remove VLAN assignments from role configurations on the gateways.

D. Configure the UBT solution to use VLAN extend mode.

Correct Answer: C

The UBT solution requires that the VLAN assignments for the wired clients are done by the gateway, not by the switch. Therefore, the role configurations on the gateways should not have any VLAN assignments, as they would override the VLAN 20 that is specified in the enforcement profile. Instead, the role configurations should only have policies that define the access rights for the clients in the "eth-internet" role. This way, the gateway can assign the clients to VLAN 20 and apply the appropriate policies based on their role

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):

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.

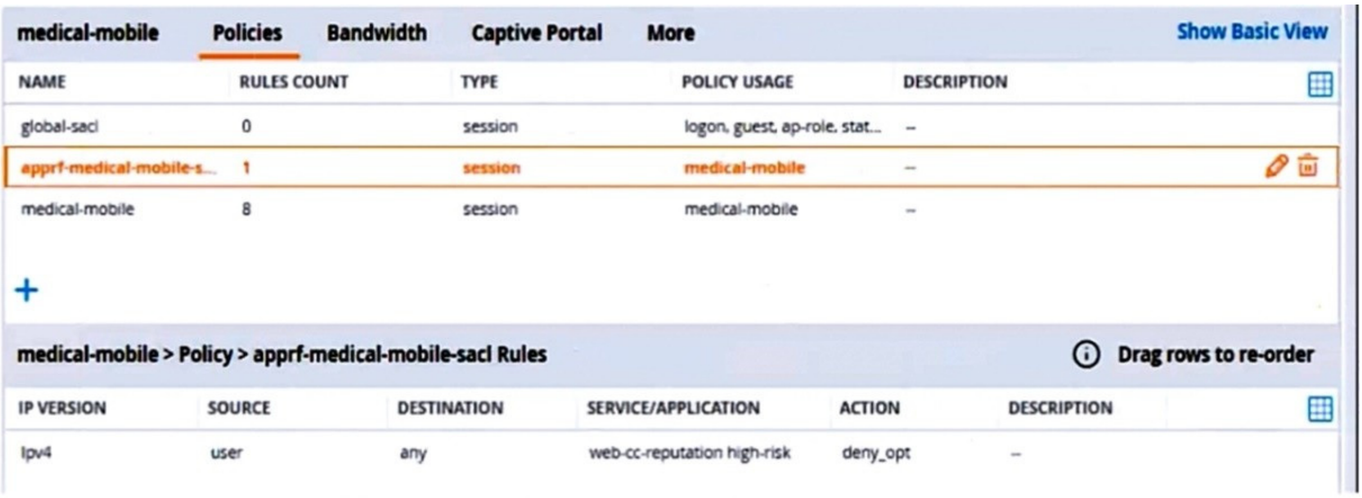
Denied access to the WLAN for a period of time if they send any Telnet traffic

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.

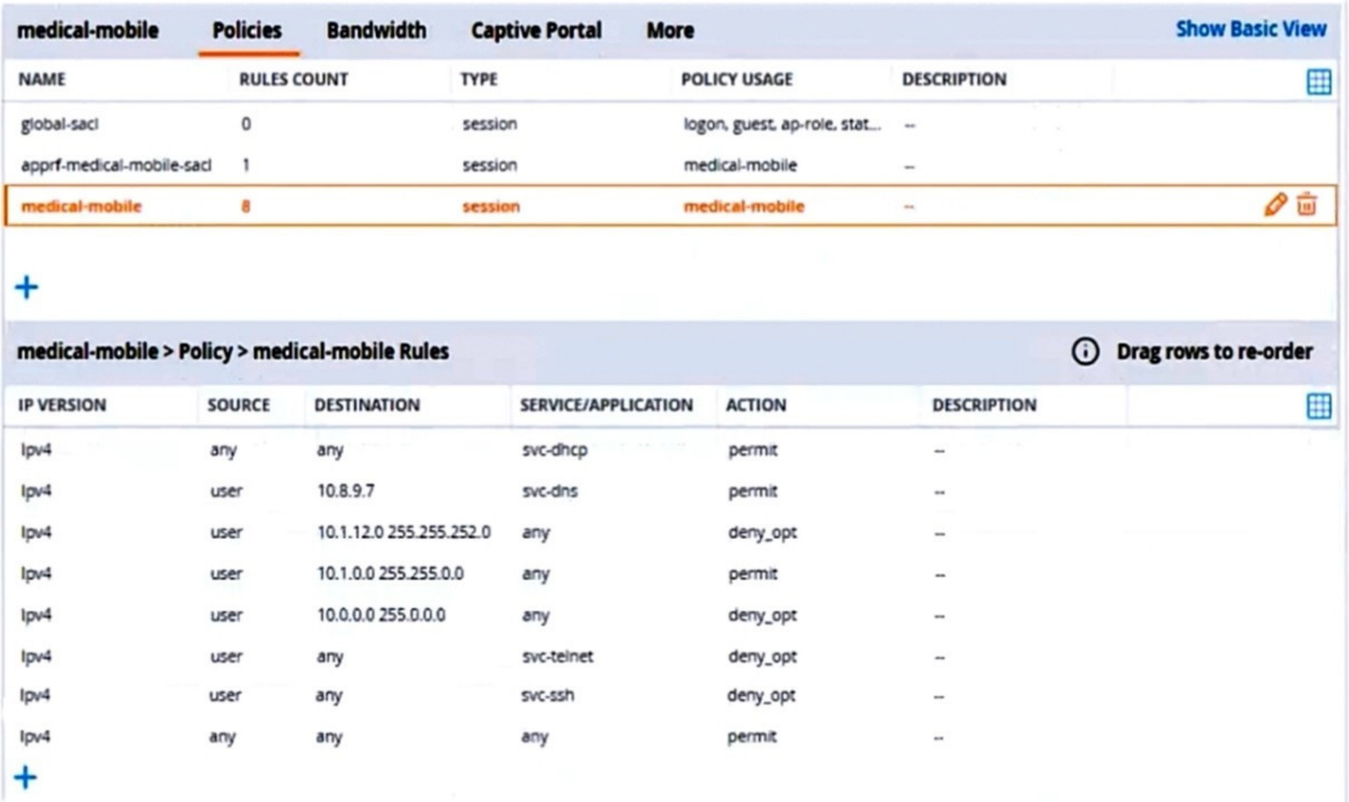


NAME	RULES COUNT	TYPE	POLICY USAGE	DESCRIPTION
global-sacl	0	session	logon, guest, ap-role, stat...	--
apprf-medical-mobile-s...	1	session	medical-mobile	--
medical-mobile	8	session	medical-mobile	--

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 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.

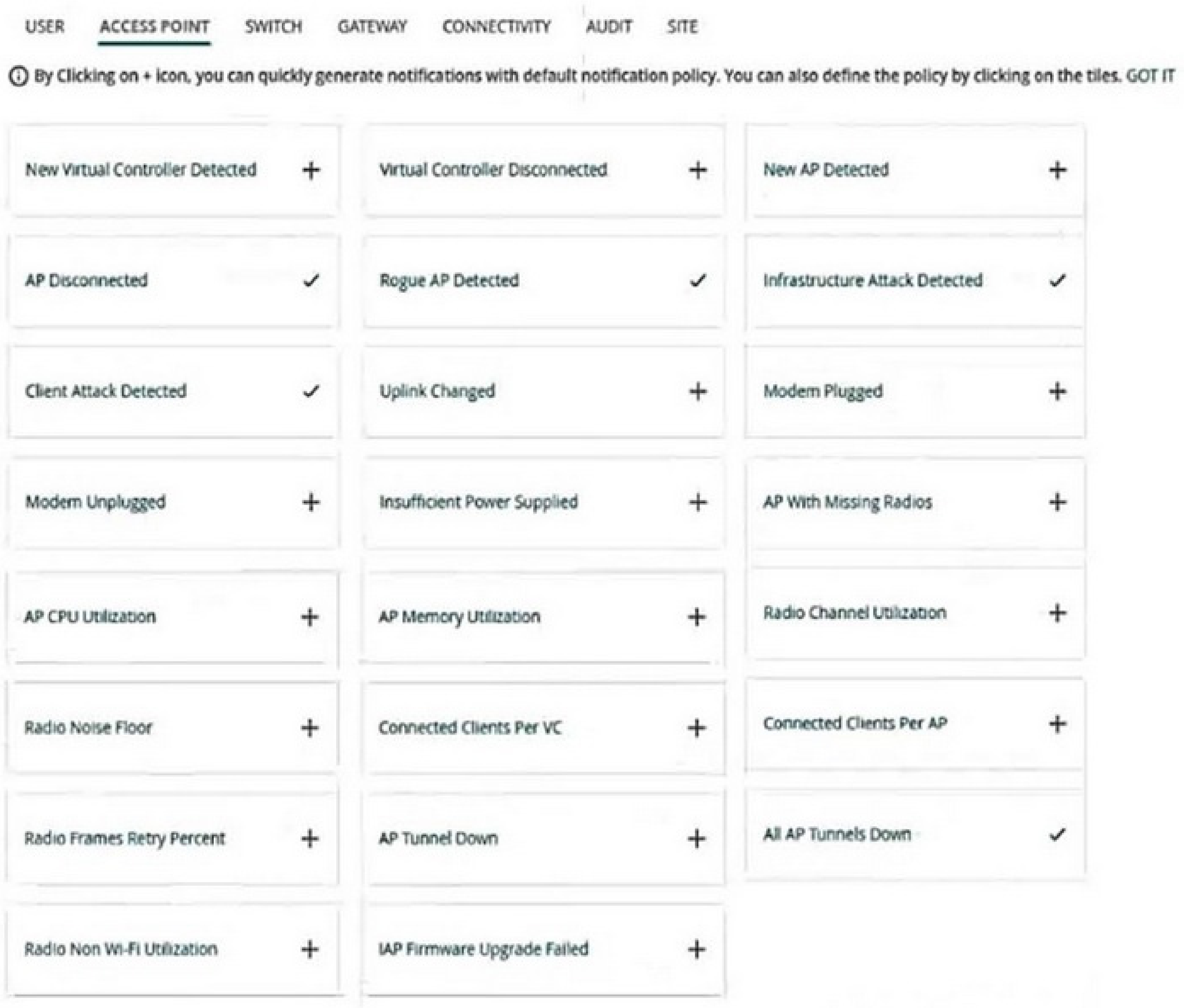
D. Move the rule in the "apprf-medical-mobile-sacl" policy between rules 7 and 8 in the "medical-mobile" policy.

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 6

A customer has an AOS 10 architecture, which includes Aruba APs. Admins have recently enabled WIDS at the high level. They also enabled alerts and email notifications for several events, as shown in the exhibit.



ⓘ By Clicking on + icon, you can quickly generate notifications with default notification policy. You can also define the policy by clicking on the tiles. GOT IT

New Virtual Controller Detected +	Virtual Controller Disconnected +	New AP Detected +
AP Disconnected ✓	Rogue AP Detected ✓	Infrastructure Attack Detected ✓
Client Attack Detected ✓	Uplink Changed +	Modem Plugged +
Modem Unplugged +	Insufficient Power Supplied +	AP With Missing Radios +
AP CPU Utilization +	AP Memory Utilization +	Radio Channel Utilization +
Radio Noise Floor +	Connected Clients Per VC +	Connected Clients Per AP +
Radio Frames Retry Percent +	AP Tunnel Down +	All AP Tunnels Down ✓
Radio Non Wi-Fi Utilization +	IAP Firmware Upgrade Failed +	

Admins are complaining that they are getting so many emails that they have to ignore them, so they are going to turn off all notifications.

What is one step you could recommend trying first?

A. Send the email notifications directly to a specific folder, and only check the folder once a week.

B. Disable email notifications for Roque AP, but leave the Infrastructure Attack Detected and Client Attack Detected notifications on.

C. Change the WIDS level to custom, and enable only the checks most likely to indicate real threats.

D. Disable just the Rogue AP and Client Attack Detected alerts, as they overlap with the Infrastructure Attack Detected alert.

Correct Answer: C

According to the AOS 10 documentation1, WIDS is a feature that monitors the radio spectrum for the presence of unauthorized, rogue access points and the use of wireless attack tools. WIDS can be configured at different levels, such as low, medium, high, or custom. The higher the level, the more checks are enabled and the more alerts are generated. However, not all checks are equally relevant or indicative of real threats. Some checks may generate false positives or unnecessary alerts that can overwhelm the administrators and reduce the effectiveness of WIDS. Therefore, one step that could be recommended to reduce the number of email notifications is to change the WIDS level to custom, and enable only the checks most likely to indicate real threats. This way, the administrators can fine-tune the WIDS settings to suit their network environment and security needs, and avoid getting flooded with irrelevant or redundant alerts. Option C is the correct answer. Option A is incorrect because sending the email notifications directly to a specific folder and only checking the folder once a week is not a good practice for security management. This could lead to missing or ignoring important alerts that require immediate attention or action. Moreover, this does not solve the problem of getting too many emails in the first place. Option B is incorrect because disabling email notifications for Rogue AP, but leaving the Infrastructure Attack Detected and Client Attack Detected notifications on, is not a sufficient solution. Rogue APs are unauthorized access points that can pose a serious security risk to the network, as they can be used to intercept or steal sensitive data, launch attacks, or compromise network performance. Therefore, disabling email notifications for Rogue APs could result in missing critical alerts that need to be addressed. Option D is incorrect because disabling just the Rogue AP and Client Attack Detected alerts, as they overlap with the Infrastructure Attack Detected alert, is not a valid assumption. The Infrastructure Attack Detected alert covers a broad range of attacks that target the network infrastructure, such as deauthentication attacks, spoofing attacks, denial-of-service attacks, etc. The Rogue AP and Client Attack Detected alerts are more specific and focus on detecting and classifying rogue devices and clients that may be involved in such attacks. Therefore, disabling these alerts could result in losing valuable information about the source and nature of the attacks.

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

Correct Answer: D

The correct answer is D. Enabling alerts and email notifications for events related to gateway IPS engine utilization and errors. 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 1. The Fail Strategy is a setting that determines how the gateways handle traffic when the IPS engine fails or crashes 2. 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 2. 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 2. To minimize this risk, it is recommended to enable alerts and email notifications for events related to gateway IPS engine utilization and errors 3. This way, the network administrators can be informed of any issues with the IPS engine and take appropriate actions to restore or troubleshoot it 3. The other options are not correct or relevant for this issue: Option A is not correct because configuring a relatively high threshold for the gateway threat count alerts would not help minimize unexpected outages caused by using the Block option. The gateway threat count alerts are used to notify the network administrators of the number of threats detected by the IPS engine, but they do not affect how the gateways handle traffic when the IPS engine fails 4. Option B is not correct because making sure that the gateways have formed a cluster and operate in default gateway mode would not help minimize unexpected outages caused by using the Block option. The gateway cluster mode is used to provide high availability and load balancing for the gateways, but it does not affect how the gateways handle traffic when the IPS engine fails . The default gateway mode is used to enable routing and NAT functions on the gateways, but it does not affect how the gateways handle traffic when the IPS engine fails . Option C is not correct because setting the IDS or IPS policy to the least restrictive option, Lenient, would not help minimize unexpected outages caused by using the Block option. The IDS or IPS policy is used to define what rules are applied by the IPS engine to inspect and block traffic, but it does not affect how the gateways handle traffic when the IPS engine fails 2. The Lenient option contains fewer and older rules than the Moderate or Strict options, which means that it

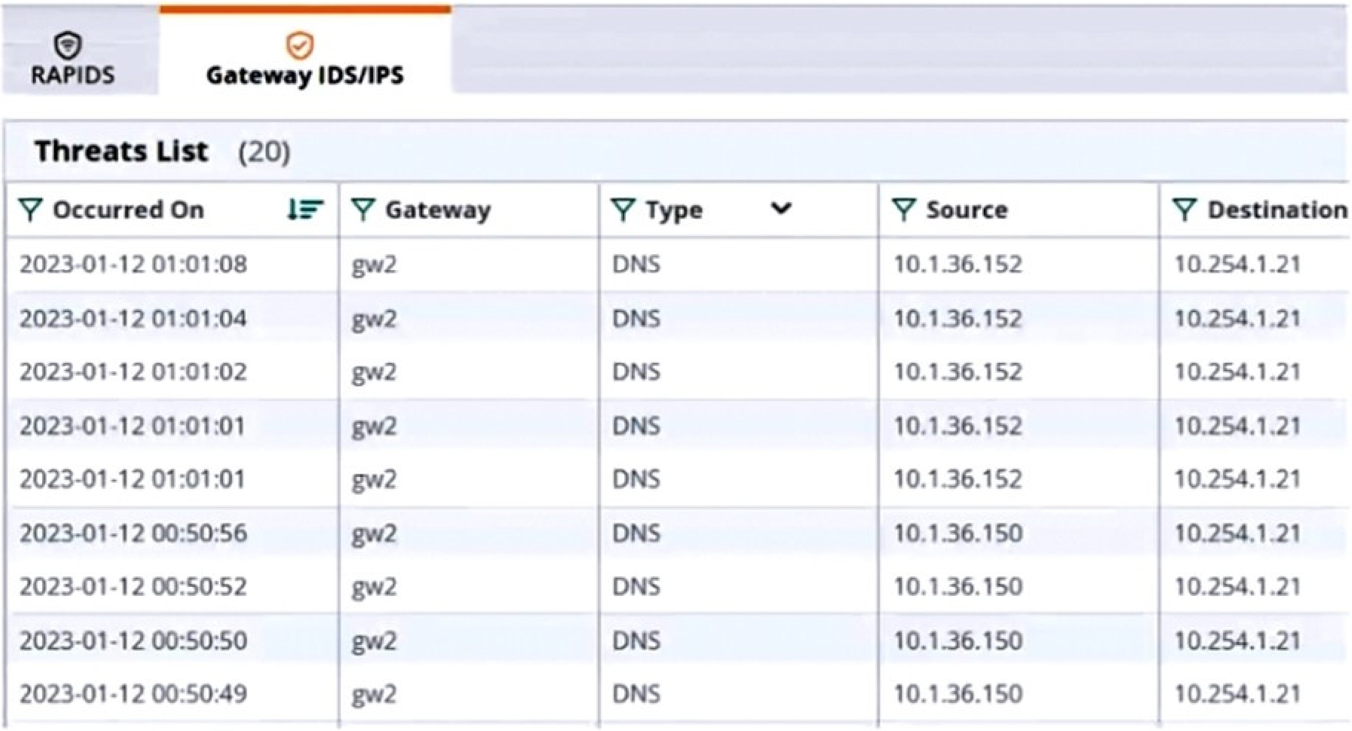
provides less security and more false negatives .

QUESTION 8

Refer to the scenario.

A hospital has an AOS10 architecture that is managed by Aruba Central. The customer has deployed a pair of Aruba 9000 Series gateways with Security licenses at each clinic. The gateways implement IDS/IPS in IDS mode.

The Security Dashboard shows these several recent events with the same signature, as shown below:



Threats List (20)

Occurred On	Gateway	Type	Source	Destination
2023-01-12 01:01:08	gw2	DNS	10.1.36.152	10.254.1.21
2023-01-12 01:01:04	gw2	DNS	10.1.36.152	10.254.1.21
2023-01-12 01:01:02	gw2	DNS	10.1.36.152	10.254.1.21
2023-01-12 01:01:01	gw2	DNS	10.1.36.152	10.254.1.21
2023-01-12 01:01:01	gw2	DNS	10.1.36.152	10.254.1.21
2023-01-12 00:50:56	gw2	DNS	10.1.36.150	10.254.1.21
2023-01-12 00:50:52	gw2	DNS	10.1.36.150	10.254.1.21
2023-01-12 00:50:50	gw2	DNS	10.1.36.150	10.254.1.21
2023-01-12 00:50:49	gw2	DNS	10.1.36.150	10.254.1.21

Which step could give you valuable context about the incident?

A. View firewall sessions on the APs and record the threat sources\\' type and OS.

B. View the user-table on APs and record the threat sources\\' 802.11 settings.

C. View the RAPIDS Security Dashboard and see if the threat sources are listed as rogues.

D. Find the Central client profile for the threat sources and note their category and family.

Correct Answer: C

The RAPIDS Security Dashboard is a feature of Aruba Central that provides a comprehensive view of the network security status, including IDS/IPS events, rogue APs, and wireless intrusion detection. By viewing the RAPIDS Security Dashboard, you can see if the threat sources are rogue APs that are spoofing legitimate DNS servers or clients. This can give you valuable context about the incident and help you identify the root cause of the attack1 Reference: Aruba Central User Guide

QUESTION 9

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.

The customer wants you to configure CPPM to collect information from Intune on demand during the authentication process.

What should you tell the Intune admins about the certificates issued to clients?

A. They must be issued by a well-known, trusted CA.

B. They must include the Intune ID in the subject name.

C. They must include the client MAC address in the subject name.

D. They must be issued by a ClearPass Onboard CA.

Correct Answer: B

To configure CPPM to collect information from Intune on demand during the authentication process, you need to use the Intune extension for ClearPass. This extension allows ClearPass to query Intune for device compliance and configuration information using the Intune API. To use this extension, you need to register an app in Azure AD and grant it the required permissions to access Intune1 The Intune extension uses the device ID as the key to query Intune for device information. The device ID is a unique identifier that is assigned by Intune to each enrolled device. The device ID can be obtained from the client certificate that is used for EAP-TLS authentication. Therefore, the certificates issued to clients must include the Intune ID in the subject name, so that ClearPass can extract it and use it to query Intune2 The certificates issued to clients do not need to be issued by a well-known, trusted CA, as long as ClearPass trusts the CA that issued them. The certificates do not need to include the client MAC address in the subject name, as this is not relevant for querying Intune. The certificates do not need to be issued by a ClearPass Onboard CA, as this is not a requirement for using the Intune extension. Reference:

1: ClearPass Extensions - Microsoft Intune Integration - Aruba, section "Configuring Microsoft Extension in ClearPass"

2: ClearPass Extensions - Microsoft Intune Integration - Aruba, section "Configuring EAP-TLS Authentication"

QUESTION 10

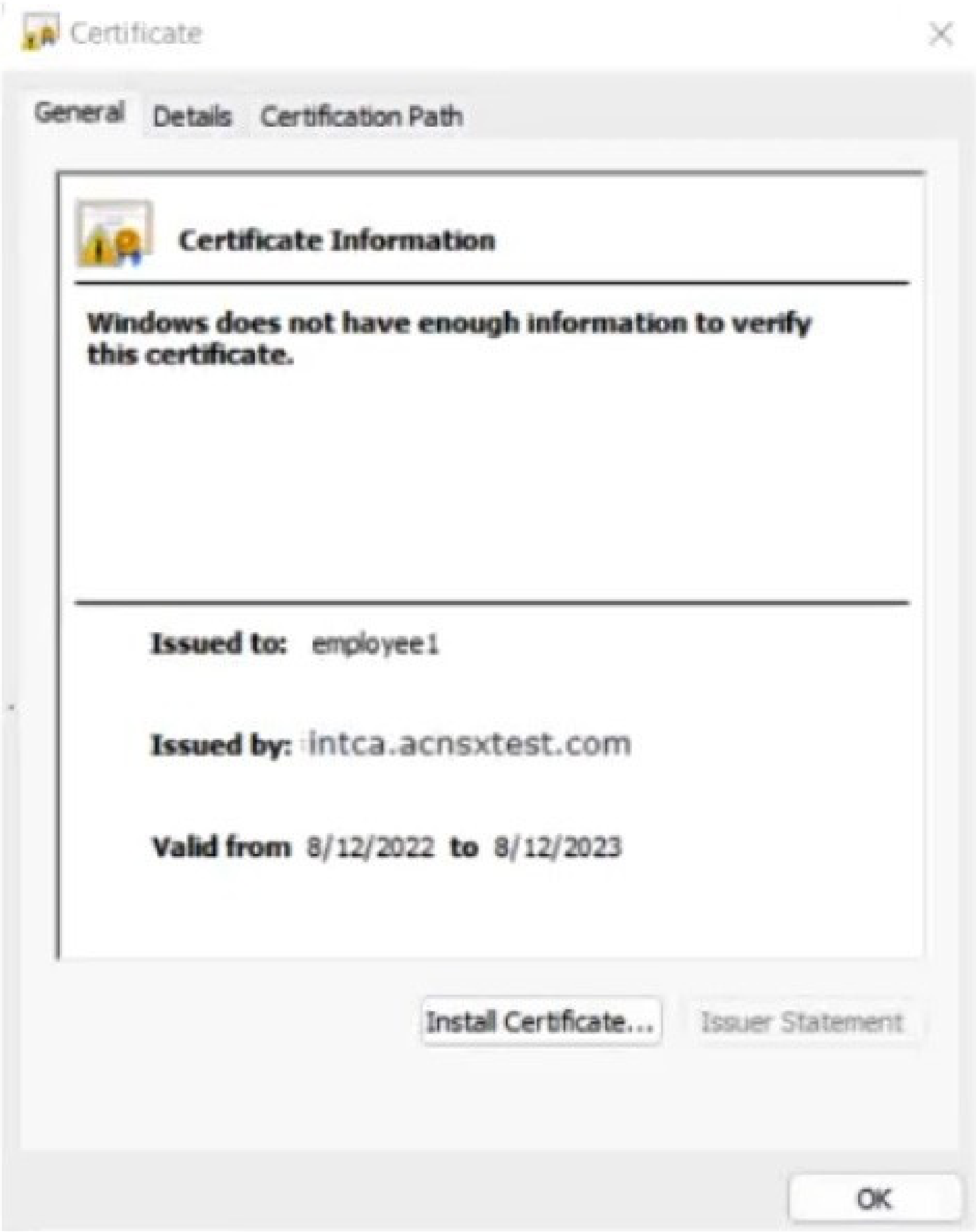
Refer to the scenario.

# 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.



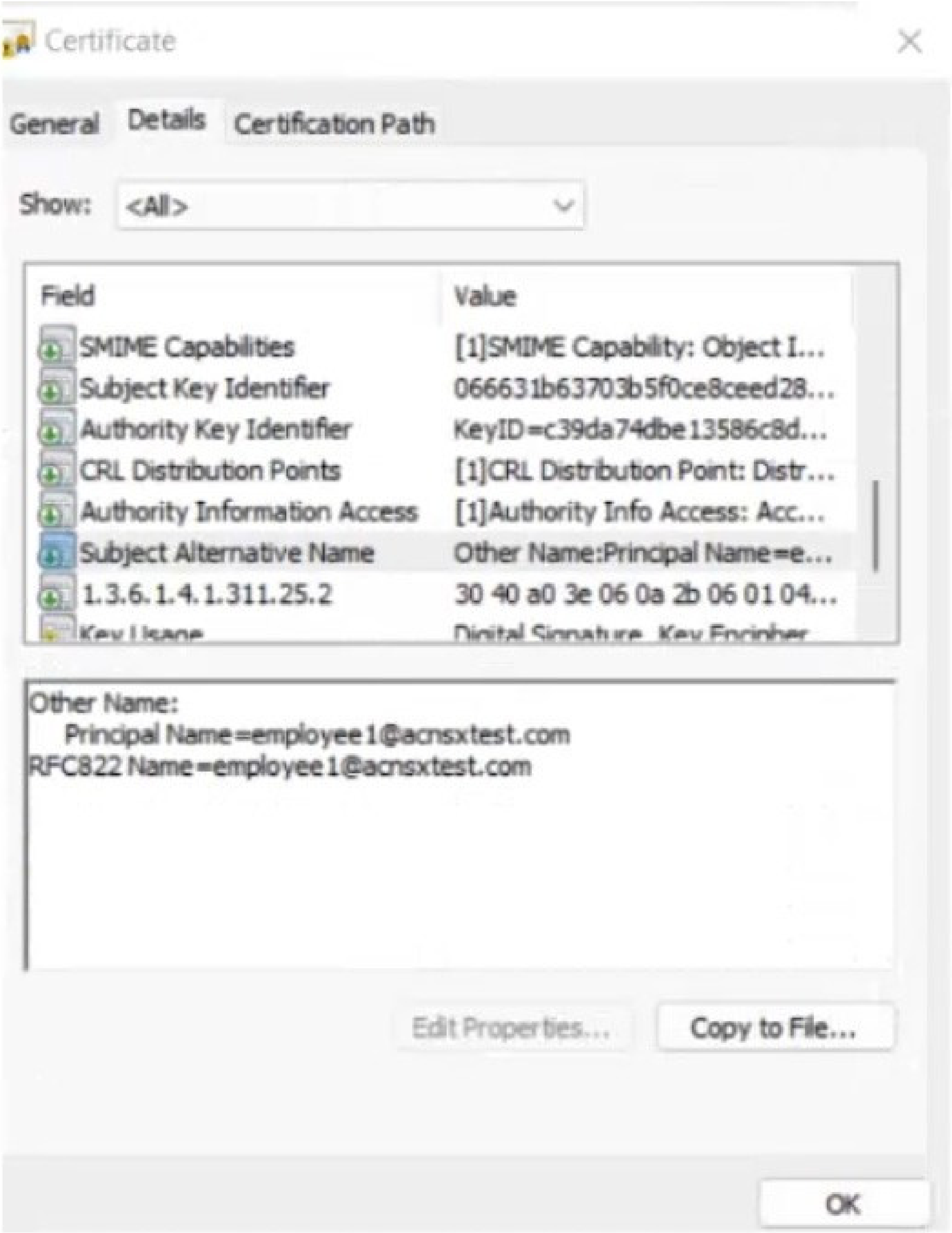
Certificate Information

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



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

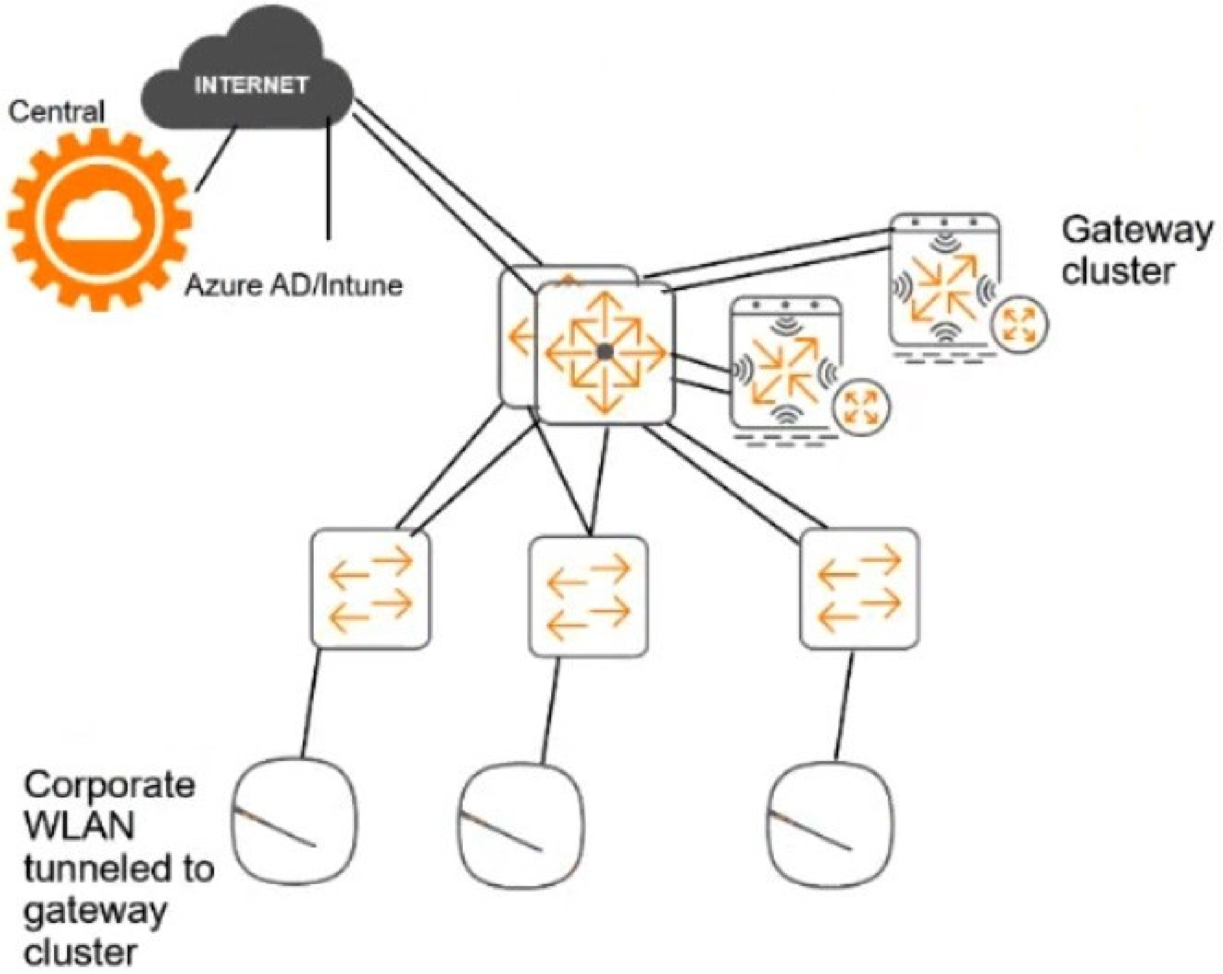
5.

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

The customer has now decided that it needs CPPM to assign certain mobile-onboarded devices to a "nurse-call" AOS user role. These are mobile-onboarded devices that are communicating with IP address 10.1.18.12 using port 4343.

What are the prerequisites for fulfilling this requirement?

A. Setting up traffic classes and role mapping rules within Central\\'s global settings

B. Creating server-based role assignment rules on APs that apply roles to clients based on traffic destinations

C. Creating server-based role assignment rules on gateways that apply roles to clients based on traffic destinations

D. Creating a tag on Central to select the proper destination connection and integrating CPPM with Device Insight

Correct Answer: C