KillTest

質量更高　服務更好

學習資料

http://www.killtest.net

一年免費更新服務

Exam : **HPE7-A10**

Title : HPE Network Security Expert Written Exam

Version : DEMO

1.A client is connected to an AOS-CX switch, which tunnels the client's traffic to an AOS-10 gateway. The gateway assigns the client to a role with these rules: any any svc-dhcp permit user alias hostl svc-dns permit user alias net1 svc-https permit user alias net2 tcp 8086 permit user alias net3 any deny user alias net4 svc-https permit.
The gateway has these aliases defined:
- host1 = 10.0.6.8
- net1 = 10.0.0.0 255.255.252.0
- net2 = 10.0.3.0 255.255.255.0
- net3 = 10.0.0.0 255.255.248.0
- net4 = 10.0.0.0 255.255.0.0 The client sends two packets:
- 1: tcp 8086 to 10.0.3.75
- 2: https to 10.0.7.24
What happens?
A. Both are denied.
B. Both are permitted.
C. The first is denied, and the second is permitted.
D. The first is permitted, and the second is denied.
Answer: D

2.You are designing an AOS-10 architecture and ClearPass solution for a manufacturing company. The company that has legacy equipment that is only WPA2 capable. You need to enhance security for these devices.
This equipment will connect to an SSID named "Factory." If the equipment passes authentication and receives custom Device Category "Manufacturing," it should receive this AOS user role: "equipment." That role and a "profiling" role for unprofiled devices are already configured on the AOS devices.
The users responsible for configuring PSKs on the equipment belong to the "FactoryAdmins" group in the company's Active Directory domain.
CPPM has an authentication source for that domain named MyAD.
As part of the solution, you have created these services on CPPM:
- Service 1:
- Type: Application
- Authentication source: MyAD
- Authorization source: None
- Enforcement policy:
- Rule 1 condition: Authorization: Endpoints Repository: Category EQUALS Manufacturing
- Rule 1 profile list: Enforcement profiles that permit application access and assign the Guest Operators role
- Default action: Deny access
- Service 2
- Type: Wireless with mPSK
- Authentication source: Guest Devices Repository
- Authorization source: None
- Enforcement policy:
- Rule 1 condition: Endpoint Device Insight Tag EQUALS Manufacturing

- Rule 1 profile list: Enforcement profile that assigns Aruba-User-Role = equipment and [Registered Device MPSK] profile
- Rule 2 condition: Endpoint: Device Insight Tag NOT_EXISTS
- Rule 2 profile list: Enforcement profile that assigns Aruba-User-Role = profiling and [Registered Device MPSK] profile
- Default action: Deny access

What is an error in this configuration?

A. Service 2 requires the Endpoints Repository as an authorization source and adjustments to the enforcement policy.

B. Service 1 uses the wrong service type.

C. Service 2 uses the wrong authentication source.

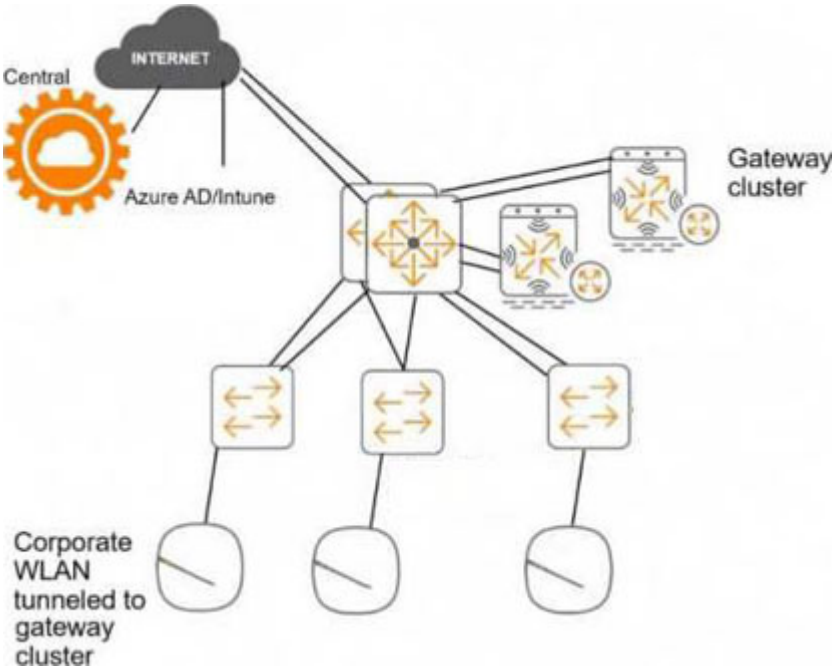
D. Service 2 is missing a necessary rule in the enforcement policy.

Answer: A

3.# Introduction to the customer

You are helping a company add HPE Aruba Networking ClearPass to their network, which uses HPE Aruba Networking 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.



ClearPass cluster IP addressing and hostnames

A customer's ClearPass cluster has these IP addresses:

• Publisher = 10.47.47.5

• Subscriber 1 = 10.47.47.6

• Subscriber 2 = 10.47.47.7

• Virtual IP with Subscriber 1 and Subscriber 2 = 10.47.47.8 The customer's DNS server has these entries

• cp.acnsxtest.com = 10.47.47.5

• cps1.acnsxtest.com = 10.47.47.6

• cps2.acnsxtest.com = 10.47.47.7

• radius.acnsxtest.com = 10.47.47.8

• onboard.acnsxtest.com = 10.47.47.8

Refer to the scenario.

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. LDAP and HPE Aruba Networking infrastructure

B. EAP and AD/LDAP Server

C. Radsec and HPE Aruba Networking infrastructure

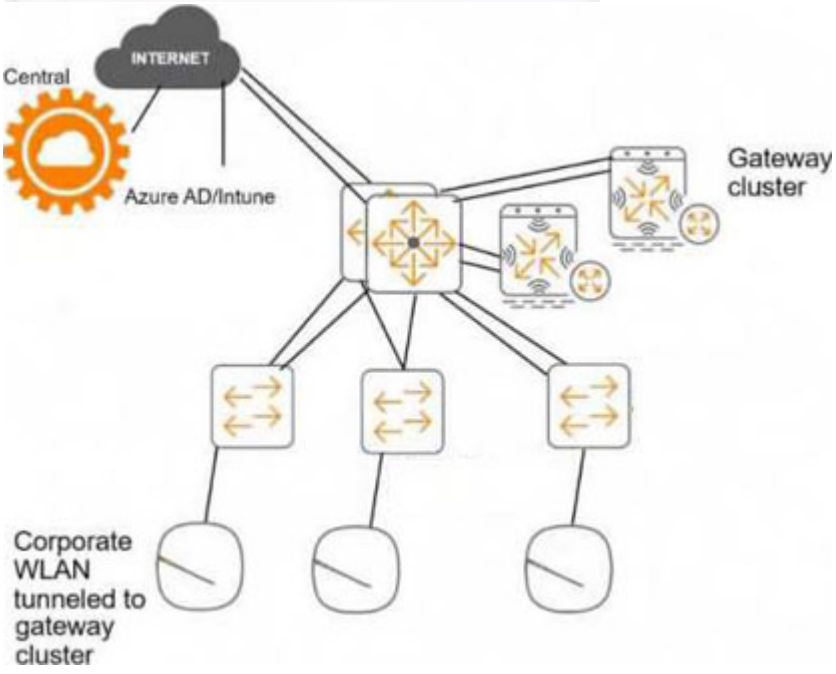
D. EAP and Radsec

Answer: B

4.# Introduction to the customer

You are helping a company add HPE Aruba Networking ClearPass to their network, which uses HPE Aruba Networking 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.



ClearPass cluster IP addressing and hostnames

A customer's ClearPass cluster has these IP addresses:

• Publisher = 10.47.47.5

• Subscriber 1 = 10.47.47.6

• Subscriber 2 = 10.47.47.7

• Virtual IP with Subscriber 1 and Subscriber 2 = 10.47.47.8 The customer's DNS server has these entries

• cp.acnsxtest.com = 10.47.47.5

• cps1.acnsxtest.com = 10.47.47.6

• cps2.acnsxtest.com = 10.47.47.7

• radius.acnsxtest.com = 10.47.47.8

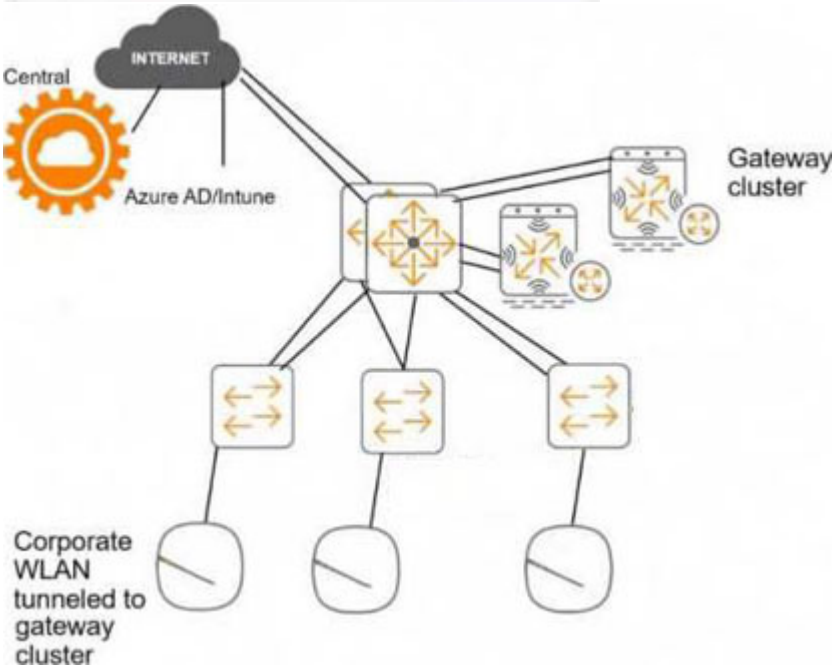
• onboard.acnsxtest.com = 10.47.47.8

Refer to the scenario.
You have started to create a CA to meet the customer's requirements for issuing certificates to mobile clients, as shown in the exhibit below.

What change will help to meet those requirements and the requirements for authenticating clients?
A. Change the EST authentication method to use an external validator.
B. Change the EST Digest Algorithm to SHA-512.
C. Recreate the CA as a registration authority under Microsoft Entra ID (Azure AD).
D. Specify an OCSP responder, setting the hostname to localhost.
Answer: D

5.# Introduction to the customer

You are helping a company add HPE Aruba Networking ClearPass to their network, which uses HPE Aruba Networking 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.



ClearPass cluster IP addressing and hostnames
A customer's ClearPass cluster has these IP addresses:
• Publisher = 10.47.47.5
• Subscriber 1 = 10.47.47.6
• Subscriber 2 = 10.47.47.7
• Virtual IP with Subscriber 1 and Subscriber 2 = 10.47.47.8 The customer's DNS server has these entries

• cp.acnsxtest.com = 10.47.47.5
• cps1.acnsxtest.com = 10.47.47.6
• cps2.acnsxtest.com = 10.47.47.7
• radius.acnsxtest.com = 10.47.47.8
• onboard.acnsxtest.com = 10.47.47.8

Refer to the scenario.

Assume that you have set up CPPM to assign HPE Aruba Networking ClearPass roles and AOS user roles as indicated in the scenario. However, a penetration tester was able to access the network with medical staff privileges on a client with a valid computer certificate but revoked medical user certificate. In this circumstance, the customer wants the client to receive computer-only access.

What can you do to correct this issue while still meeting the other customer requirements?

A. Add a role mapping rule that assigns clients that have failed TEAP Method 2 to a "user-failed" role. Add an enforcement policy rule to the top of the list that assigns clients with the "domain-computer" and "user-failed" roles to the "computer-only" profile.

B. Check the order of the enforcement policy rules. Make sure that any rule that applies the "computer-only" profile is at the top of the list. Also, ensure that the default rule is the drop access profile.

C. Change the authentication method configuration to use CRLs to validate certificates' status instead of OCSP.

D. Adjust the authentication filter used in the authentication source. Change any references to the %{Username} variable to the %{TEAP-Method-2-Username} variable.

Answer: A