Interactive HPE6-A78 Course | Valid HPE6-A78 Exam Tutorial

P.S. Free 2026 HP HPE6-A78 dumps are available on Google Drive shared by Pass4sures: https://drive.google.com/open?id=10PO41zzCjzoOmOsb-L5t9pbtvrzXn_aM

Once the user has used our HPE6-A78 test prep for a mock exercise, the product's system automatically remembers and analyzes all the user's actual operations. The user must complete the test within the time specified by the simulation system, and there is a timer on the right side of the screen, as long as the user begins the practice of HPE6-A78 Quiz guide, the timer will run automatic and start counting. The transfer can be based on the HPE6-A78 valid practice questions report to develop a learning plan that meets your requirements. As long as you study with our HPE6-A78 exam questions, you will pass the exam.

To become Aruba Certified Network Security Associate, you must pass the HPE6-A78 certification exam. HPE6-A78 exam consists of 60 multiple-choice questions that must be completed within 90 minutes. HPE6-A78 exam is graded on a scale of 1000, with a minimum passing score of 720 required to earn the certification. Additionally, candidates are required to have a valid Aruba Certified Mobility Associate (ACMA) certification as a prerequisite for taking the HPE6-A78 exam. The Aruba Certified Network Security Associate certification is recognized globally and is highly valued by organizations that use Aruba technologies.

HP HPE6-A78 certification exam covers a broad range of topics related to network security, including access control and authentication, firewall and intrusion prevention, VPN technologies, wireless security, and network security management. HPE6-A78 Exam is designed to test the knowledge and skills of candidates in these areas, and successful candidates will demonstrate their ability to design and implement secure network infrastructures. Overall, the HP HPE6-A78 certification is an excellent way for IT professionals to demonstrate their expertise in network security and advance their careers in this important field.

HP HPE6-A78 exam covers a wide range of topics related to wireless network security, including authentication methods, encryption techniques, firewall configuration, and intrusion prevention. HPE6-A78 exam is designed to test the candidate's understanding of these topics and their ability to apply this knowledge in real-world situations.

>> Interactive HPE6-A78 Course <<

Valid HPE6-A78 Exam Tutorial - HPE6-A78 Cert Exam

To attempt the HP HPE6-A78 exam optimally and ace it on the first attempt, proper exam planning is crucial. Since the HP HPE6-A78 exam demands a lot of time and effort, we designed the HP HPE6-A78 Exam Dumps in such a way that you would not have to go through sleepless study nights or disturb your schedule.

HP Aruba Certified Network Security Associate Exam Sample Questions (Q131-Q136):

NEW QUESTION # 131
What correctly describes the Pairwise Master Key (PMK) in thee specified wireless security protocol?

- A. In WPA3-Personal, the PMK is unique per session and derived using Simultaneous Authentication of Equals.

- B. In WPA3-Enterprise, the PMK is unique per session and derived using Simultaneous Authentication of Equals.
- C. In WPA3-Personal, the PMK is derived directly from the passphrase and is the same tor every session.
- D. In WPA3-Personal, the PMK is the same for each session and is communicated to clients that authenticate

Answer: B

Explanation:
In WPA3-Enterprise, the Pairwise Master Key (PMK) is indeed unique for each session and is derived using a process called Simultaneous Authentication of Equals (SAE). SAE is a new handshake protocol available in WPA3 that provides better security than the Pre-Shared Key (PSK) used in WPA2. This handshake process strengthens user privacy in open networks and provides forward secrecy. The information on SAE and its use in generating a unique PMK can be found in the Wi-Fi Alliance's WPA3 specifications and related technical documentation.

NEW QUESTION # 132
A customer has an AOS-10 network infrastructure. The customer is looking for a solution that can classify many different types of devices, including IoT devices. Which solution should you explain can provide these capabilities?

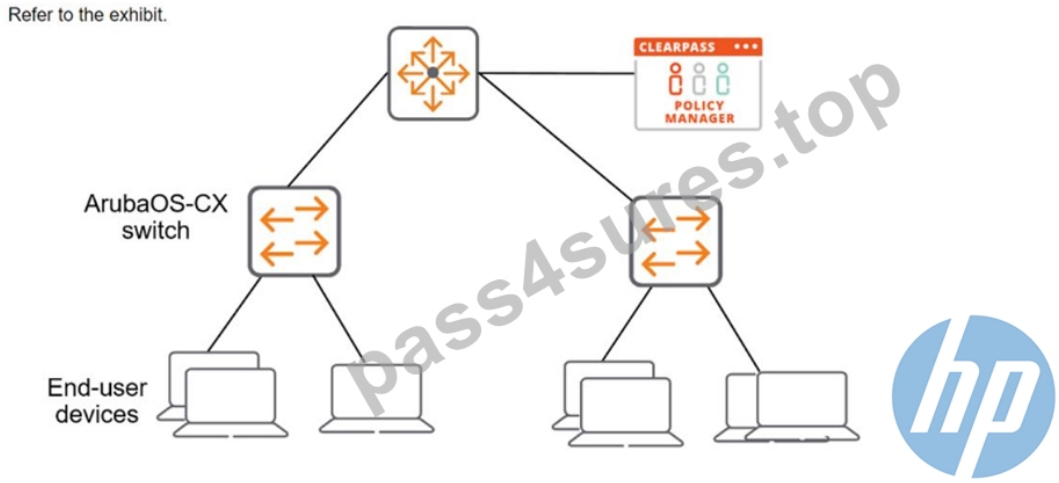
- A. HPE Aruba Networking ClearPass Onboard
- B. HPE Aruba Networking ClearPass OnGuard
- C. HPE Aruba Networking Central
- D. HPE Aruba Networking EdgeConnect SD-WAN

Answer: B

Explanation:
HPE Aruba Networking ClearPass OnGuard: This is a component of the ClearPass Policy Manager platform specifically designed for endpoint posture assessment and health checks. It can identify and classify a wide range of devices connecting to the network, including traditional endpoints, mobile devices, and importantly, IoT devices. It analyzes device attributes and behaviors to determine their type and security posture.
Let's look at why the other options are less suitable for this specific requirement:
HPE Aruba Networking EdgeConnect SD-WAN: This solution focuses on optimizing wide area network (WAN) connectivity, improving application performance, and providing secure branch-to-branch and branch-to-cloud connections. While it can identify traffic from different devices, its primary function isn't detailed device classification at the network access layer.
HPE Aruba Networking Central: This is a cloud-based network management platform that provides visibility, configuration, and management for Aruba network devices (APs, switches, gateways). While it offers insights into connected devices, its core function isn't the deep classification of diverse endpoint types like IoT devices.
HPE Aruba Networking ClearPass Onboard: This component of ClearPass Policy Manager focuses on simplifying the secure onboarding of personal or unmanaged devices (BYOD). While it involves device identification during the onboarding process, its primary goal isn't continuous and comprehensive classification of all device types, especially the detailed classification needed for diverse IoT devices.
Therefore, HPE Aruba Networking ClearPass OnGuard is the most appropriate solution for classifying a wide range of devices, including IoT devices, within an AOS-10 network infrastructure.

NEW QUESTION # 133
Refer to the exhibit.

Refer to the exhibit.



What is another setting that you must configure on the switch to meet these requirements?

- A. Configure a CPPM username and password that match a CPPM admin account.
- B. Disable SSH on the default VRF and enable it on the mgmt VRF instead.
- C. Create port-access roles with the same names of the roles that CPPM will send in Aruba-Admin-Role VSAs.
- D. Set the aaa authentication login method for SSH to the "radius" server-group (with local as backup).

Answer: D

Explanation:
To meet the requirements for configuring an ArubaOS-CX switch for integration with ClearPass Policy Manager (CPPM), it is necessary to set the AAA authentication login method for SSH to use the "radius" server-group, with "local" as a backup. This ensures that when an admin attempts to SSH into the switch, the authentication request is first sent to CPPM via RADIUS. If CPPM is unavailable, the switch will fall back to using local authentication12.
Here's why the other options are not correct:
Option B is incorrect because configuring a CPPM username and password on the switch that matches a CPPM admin account is not required for SSH login; rather, the switch needs to be configured to communicate with CPPM for authentication.
Option C is incorrect because while CPPM will send Aruba-Admin-Role Vendor-Specific Attributes (VSAs), the switch does not need to have port-access roles created with the same names; it needs to interpret the VSA to assign the correct role.
Option D is incorrect because disabling SSH on the default VRF and enabling it on the mgmt VRF is not related to the authentication process with CPPM.
Therefore, the correct answer is A, as setting the AAA authentication login method for SSH to the "radius" server-group with "local" as backup is a key step in ensuring that the switch can authenticate admins through CPPM while providing a fallback method12.

NEW QUESTION # 134
A client has accessed an HTTPS server at myhost1.example.com using Chrome. The server sends a certificate that includes these properties:
Subject name: myhost.example.com
SAN: DNS: myhost.example.com; DNS: myhost1.example.com
Extended Key Usage (EKU): Server authentication
Issuer: MyCA_Signing
The server also sends an intermediate CA certificate for MyCA_Signing, which is signed by MyCA. The client's Trusted CA Certificate list does not include the MyCA or MyCA_Signing certificates.
Which factor or factors prevent the client from trusting the certificate?

- A. The certificate lacks a valid SAN, and the client does not have the correct trusted CA certificates.
- B. The certificate lacks a valid SAN.
- C. The certificate lacks the correct EKU.
- D. The client does not have the correct trusted CA certificates.

Answer: D

Explanation:
When a client (e.g., a Chrome browser) accesses an HTTPS server, the server presents a certificate to establish a secure connection. The client must validate the certificate to trust the server. The certificate in this scenario has the following properties:

Subject name: myhost.example.com
SAN (Subject Alternative Name): DNS: myhost.example.com; DNS: myhost1.example.com Extended Key Usage (EKU): Server authentication Issuer: MyCA_Signing (an intermediate CA) The server also sends an intermediate CA certificate for MyCA_Signing, signed by MyCA (the root CA).
The client's Trusted CA Certificate list does not include MyCA or MyCA_Signing.
Certificate Validation Process:
Name Validation: The client checks if the server's hostname (myhost1.example.com) matches the Subject name or a SAN in the certificate. Here, the SAN includes "myhost1.example.com," so the name validation passes.
EKU Validation: The client verifies that the certificate's EKU includes "Server authentication," which is required for HTTPS. The EKU is correctly set to "Server authentication," so this validation passes.
Chain of Trust Validation: The client builds a certificate chain from the server's certificate to a trusted root CA in its Trusted CA Certificate list. The chain is:
Server certificate (issued by MyCA_Signing)
Intermediate CA certificate (MyCA_Signing, issued by MyCA)
Root CA certificate (MyCA, which should be in the client's trust store) The client's Trusted CA Certificate list does not include MyCA or MyCA_Signing, meaning the client cannot build a chain to a trusted root CA. This causes the validation to fail.
Option A, "The client does not have the correct trusted CA certificates," is correct. The client's trust store must include the root CA (MyCA) to trust the certificate chain. Since MyCA is not in the client's Trusted CA Certificate list, the client cannot validate the chain, and the certificate is not trusted.
Option B, "The certificate lacks a valid SAN," is incorrect. The SAN includes "myhost1.example.com," which matches the server's hostname, so the SAN is valid.
Option C, "The certificate lacks the correct EKU," is incorrect. The EKU is set to "Server authentication," which is appropriate for HTTPS.
Option D, "The certificate lacks a valid SAN, and the client does not have the correct trusted CA certificates," is incorrect because the SAN is valid, as explained above. The only issue is the missing trusted CA certificates.
The HPE Aruba Networking AOS-CX 10.12 Security Guide states:
"For a client to trust a server's certificate during HTTPS communication, the client must validate the certificate chain to a trusted root CA in its trust store. If the root CA (e.g., MyCA) or intermediate CA (e.g., MyCA_Signing) is not in the client's Trusted CA Certificate list, the chain of trust cannot be established, and the client will reject the certificate. The Subject Alternative Name (SAN) must include the server's hostname, and the Extended Key Usage (EKU) must include 'Server authentication' for HTTPS." (Page 205, Certificate Validation Section) Additionally, the HPE Aruba Networking Security Fundamentals Guide notes:
"A common reason for certificate validation failure is the absence of the root CA certificate in the client's trust store. For example, if a server's certificate is issued by an intermediate CA (e.g., MyCA_Signing) that chains to a root CA (e.g., MyCA), the client must have the root CA certificate in its Trusted CA Certificate list to trust the chain." (Page 45, Certificate Trust Issues Section)
:
HPE Aruba Networking AOS-CX 10.12 Security Guide, Certificate Validation Section, Page 205.
HPE Aruba Networking Security Fundamentals Guide, Certificate Trust Issues Section, Page 45.

NEW QUESTION # 135
A company has Aruba Mobility Controllers (MCs), Aruba campus APs, and ArubaOS-Switches. The company plans to use ClearPass Policy Manager (CPPM) to classify endpoints by type. This company is using only CPPM and no other ClearPass solutions.
The ClearPass admins tell you that they want to use HTTP User-Agent strings to help classify endpoints.
What should you do as a part of configuring the ArubaOS-Switches to support this requirement?

- A. Configure CPPM as the sFlow collector, and make sure that sFlow is enabled on edge ports.
- B. Create remote mirrors that collect traffic on edge ports, and mirror it to CPPM's IP address.
- C. Connect the switches to CPPM's span ports, and set up mirroring of HTTP traffic on the switches.
- D. Create a device fingerprinting policy that includes HTTP, and apply the policy to edge ports.

Answer: A

Explanation:
ArubaOS-Switches can use sFlow technology to sample network traffic and send the samples to a collector, such as ClearPass Policy Manager (CPPM), for analysis. sFlow can be configured to capture various types of traffic, including HTTP, which typically contains User-Agent strings that can be used for device fingerprinting and classification.
To support the requirement for using HTTP User-Agent strings to classify endpoints, the switches would need to be configured to send sFlow samples containing HTTP traffic to CPPM. CPPM would then analyze these samples and use the User-Agent strings to classify the devices.
Therefore, the correct action to configure ArubaOS-Switches would involve:

Configuring CPPM as the sFlow collector on the switches.
Enabling sFlow on the edge ports that connect to endpoints.
This approach allows the network traffic to be analyzed by CPPM without requiring any additional mirroring or redirection of traffic, which would be resource-intensive and potentially disruptive to network performance.

NEW QUESTION # 136
.....

The only aim of our company is to help each customer pass their exam as well as getting the important certification in a short time. If you want to pass your exam and get the HPE6-A78 certification which is crucial for you successfully, I highly recommend that you should choose the HPE6-A78 study materials from our company so that you can get a good understanding of the exam that you are going to prepare for. We believe that if you decide to buy the HPE6-A78 Study Materials from our company, you will pass your exam and get the certification in a more relaxed way than other people.