Trustworthy HP HPE6-A78 Pdf | HPE6-A78 Exam Prep

BTW, DOWNLOAD part of ExamDumpsVCE HPE6-A78 dumps from Cloud Storage: https://drive.google.com/open?id=165pHFQ34_a49Awqr6HkxdaDaLr8XZmsx

The HPE6-A78 PDF is the collection of real, valid, and updated Aruba Certified Network Security Associate Exam (HPE6-A78) practice questions. The HP HPE6-A78 PDF dumps file works with all smart devices. You can use the HPE6-A78 PDF questions on your tablet, smartphone, or laptop and start HPE6-A78 Exam Preparation anytime and anywhere. The HPE6-A78 dumps PDF provides you with everything that you must need in HPE6-A78 exam preparation and enable you to crack the final HPE6-A78 exam quickly.

HPE6-A78 exam is an essential certification exam for those who are interested in becoming an Aruba Certified Network Security Associate. Aruba Certified Network Security Associate Exam certification validates the knowledge and skills required to secure wireless networks using Aruba products and technologies. HPE6-A78 Exam focuses on various topics such as implementing secure network architecture, using firewall policies and rules, network access controls, and much more. HPE6-A78 exam has been designed to validate the candidate's ability to identify, analyze, and mitigate network security risks.

>> Trustworthy HP HPE6-A78 Pdf <<

Efficient HP Trustworthy HPE6-A78 Pdf & Perfect ExamDumpsVCE - Leading Provider in Qualification Exams

The HP HPE6-A78 practice exam software will provide you with feedback on your performance. The HP HPE6-A78 practice test software also includes a built-in timer and score tracker so students can monitor their progress. HPE6-A78 Practice Exam enables applicants to practice time management, answer strategies, and all other elements of the final HP HPE6-A78 certification exam and can check their scores.

HP HPE6-A78, also known as the Aruba Certified Network Security Associate (ACNSA) exam, is a certification test designed for IT professionals who want to demonstrate their knowledge and skills in network security. HPE6-A78 exam covers a range of topics related to Aruba's network security solutions, such as firewall policies, virtual private networks (VPNs), and access control. Passing the HPE6-A78 Exam is a great way to validate your expertise in network security and enhance your career prospects in the field.

HP Aruba Certified Network Security Associate Exam Sample Questions (Q141-Q146):

NEW QUESTION # 141
Which endpoint classification capabilities do Aruba network infrastructure devices have on their own without ClearPass solutions?

- A. ArubaOS-Switches can use DHCP fingerprints to construct detailed endpoint profiles.
- B. ArubaOS devices (controllers and IAPs) can use DHCP fingerprints to assign roles to clients.
- C. ArubaOS-CX switches can use a combination of active and passive methods to assign roles to clients.
- D. ArubaOS devices can use a combination of DHCP fingerprints, HTTP User-Agent strings, and Nmap to construct endpoint profiles.

Answer: B

Explanation:
Without the integration of Aruba ClearPass or other advanced network access control solutions, ArubaOS devices (controllers and Instant APs) are able to use DHCP fingerprinting to assign roles to clients. This method allows the devices to identify the type of client devices connecting to the network based on the DHCP requests they send. While this is a more basic form of endpoint classification compared to the capabilities provided by ClearPass, it still enables some level of access control based on device type. This functionality and its limitations are described in Aruba's product documentation for ArubaOS devices, highlighting the benefits of integrating a full-featured solution like ClearPass for more granular and powerful endpoint classification capabilities.

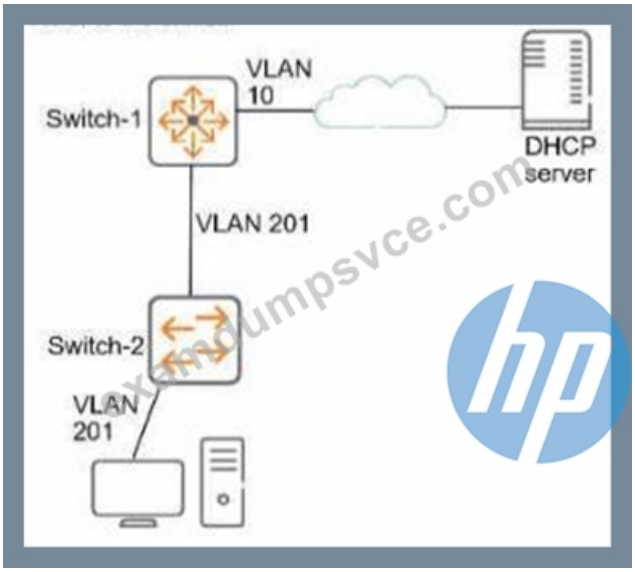
NEW QUESTION # 142
What is a benefit of Opportunistic Wireless Encryption (OWE)?

- A. It offers more control over who can connect to the wireless network when compared with WPA2-Personal.
- B. It allows both WPA2-capable and WPA3-capable clients to authenticate to the same WPA-Personal WLAN.
- C. It allows anyone to connect, but provides better protection against eavesdropping than a traditional open network.
- D. It provides protection for wireless clients against both honeypot APs and man-in-the-middle (MITM) attacks.

Answer: C

Explanation:
Opportunistic Wireless Encryption (OWE) is a WPA3 feature designed for open wireless networks, where no password or authentication is required to connect. OWE enhances security by providing encryption for devices that support it, without requiring a pre-shared key (PSK) or 802.1X authentication.
Option C, "It allows anyone to connect, but provides better protection against eavesdropping than a traditional open network," is correct. In a traditional open network (no encryption), all traffic is sent in plaintext, making it vulnerable to eavesdropping. OWE allows anyone to connect (as it's an open network), but it negotiates unique encryption keys for each client using a Diffie-Hellman key exchange. This ensures that client traffic is encrypted with AES (e.g., using AES-GCMP), protecting it from eavesdropping. OWE in transition mode also supports non-OWE devices, which connect without encryption, but OWE-capable devices benefit from the added security.
Option A, "It allows both WPA2-capable and WPA3-capable clients to authenticate to the same WPA-Personal WLAN," is incorrect. OWE is for open networks, not WPA-Personal (which uses a PSK). WPA2/WPA3 transition mode (not OWE) allows both WPA2 and WPA3 clients to connect to the same WPA-Personal WLAN.
Option B, "It offers more control over who can connect to the wireless network when compared with WPA2-Personal," is incorrect. OWE is an open network protocol, meaning it offers less control over who can connect compared to WPA2-Personal, which requires a PSK for access.
Option D, "It provides protection for wireless clients against both honeypot APs and man-in-the-middle (MITM) attacks," is incorrect. OWE provides encryption to prevent eavesdropping, but it does not protect against honeypot APs (rogue APs broadcasting the same SSID) or MITM attacks, as it lacks authentication mechanisms to verify the AP's identity. Protection against such attacks requires 802.1X authentication (e.g., WPA3-Enterprise) or other security measures.
The HPE Aruba Networking AOS-8 8.11 User Guide states:
"Opportunistic Wireless Encryption (OWE) is a WPA3 feature for open networks that allows anyone to connect without a password, but provides better protection against eavesdropping than a traditional open network. OWE uses a Diffie-Hellman key exchange to negotiate unique encryption keys for each client, ensuring that traffic is encrypted with AES-GCMP and protected from unauthorized interception." (Page 290, OWE Overview Section) Additionally, the HPE Aruba Networking Wireless Security Guide notes:
"OWE enhances security for open WLANs by providing encryption without requiring authentication. It allows any device to connect, but OWE-capable devices benefit from encrypted traffic, offering better protection against eavesdropping compared to a traditional open network where all traffic is sent in plaintext." (Page 35, OWE Benefits Section)
:
HPE Aruba Networking AOS-8 8.11 User Guide, OWE Overview Section, Page 290.
HPE Aruba Networking Wireless Security Guide, OWE Benefits Section, Page 35.

NEW QUESTION # 143
Refer to the exhibit.



This company has ArubaOS-Switches. The exhibit shows one access layer switch, Swllcn-2. as an example, but the campus actually has more switches. The company wants to slop any internal users from exploiting ARP What Is the proper way to configure the switches to meet these requirements?

- A. On Swltch-2, configure static PP-to-MAC bindings for all end-user devices on the network
- B. On Switch-2, make ports connected to employee devices trusted ports for ARP protection
- C. On Switch-1, enable ARP protection globally, and enable ARP protection on ail VLANs.
- D. On Swltch-2, enable DHCP snooping globally and on VLAN 201 before enabling ARP protection

Answer: A

NEW QUESTION # 144
What purpose does an initialization vector (IV) serve for encryption?

- A. It helps parties to negotiate the keys and algorithms used to secure data before data transmission.
- B. It enables programs to convert easily-remembered passphrases to keys of a correct length.
- C. It makes encryption algorithms more secure by ensuring that same plaintext and key can produce different ciphertext.
- D. It enables the conversion of asymmetric keys into keys that are suitable for symmetric encryption.

Answer: C

Explanation:
The primary purpose of an Initialization Vector (IV) in encryption is to ensure that the same plaintext encrypted with the same encryption key will produce different ciphertext each time it is encrypted. This variability is crucial for securing repetitive data patterns and preventing certain types of cryptographic attacks, such as replay or pattern analysis attacks. The IV adds randomness to the encryption process, making it more secure by ensuring that encrypted messages are unique, even if the plaintext and key remain unchanged. This prevents attackers from deducing patterns or inferring any useful information from repeated ciphertext.

NEW QUESTION # 145
What is one thing can you determine from the exhibits?

- A. CPPM originally assigned the client to a role for non-profiled devices. It sent a CoA to the authenticator after it categorized the device.
- B. CPPM first assigned the client to a role based on the user's identity. Then, it discovered that the client had an invalid category, so it sent a CoA to blacklist the client.
- C. CPPM was never able to determine a device category for this device, so you need to check settings in the network infrastructure to ensure they support CPPM's endpoint classification.
- D. CPPM sent a CoA message to the client to prompt the client to submit information that CPPM can use to profile it.

Answer: A

Explanation:
Based on the exhibits which seem to show RADIUS authentication and CoA logs, one can determine that CPPM (ClearPass Policy Manager) initially assigned the client to a role meant for non-profiled devices and then sent a CoA to the network access device (authenticator) once the device was categorized. This is a common workflow in network access control, where a device is first given limited access until it can be properly identified, after which appropriate access policies are applied.

NEW QUESTION # 146
.....