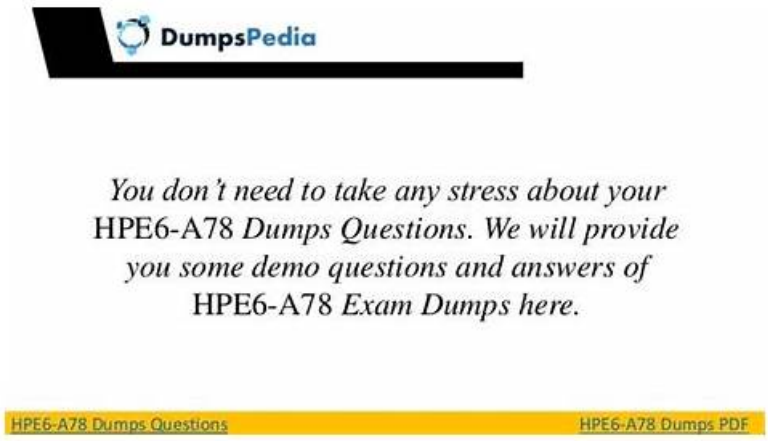
HPE6-A78 Sample Exam & HPE6-A78 Reliable Test Vce



BTW, DOWNLOAD part of PassExamDumps HPE6-A78 dumps from Cloud Storage: https://drive.google.com/open?id=1AhA1y5JoLipx-34XRCh-K1p_h73XM1Nr

Hence, if you want to sharpen your skills, and get the Aruba Certified Network Security Associate Exam (HPE6-A78) certification done within the target period, it is important to get the best Aruba Certified Network Security Associate Exam (HPE6-A78) exam questions. You must try PassExamDumps Aruba Certified Network Security Associate Exam (HPE6-A78) practice exam that will help you get the HP HPE6-A78 certification.

HP HPE6-A78 exam is a certification exam designed to test the knowledge and skills of network security professionals. HPE6-A78 exam is specifically focused on Aruba Certified Network Security Associate (ACNSA) certification, which is a widely recognized certification in the industry. HPE6-A78 Exam is designed to assess the candidate's ability to implement and maintain secure network infrastructure using Aruba products.

>> HPE6-A78 Sample Exam <<

2025 HPE6-A78 Sample Exam | Pass-Sure HPE6-A78: Aruba Certified Network Security Associate Exam 100% Pass

To address the problems of Aruba Certified Network Security Associate Exam (HPE6-A78) exam candidates who are busy, PassExamDumps has made the Aruba Certified Network Security Associate Exam (HPE6-A78) dumps PDF format of real Aruba Certified Network Security Associate Exam (HPE6-A78) exam questions. This format's feature to run on all smart devices saves your time. Because of this, the portability of Aruba Certified Network Security Associate Exam (HPE6-A78) dumps PDF aids in your preparation regardless of place and time restrictions.

HP Aruba Certified Network Security Associate Exam Sample Questions (Q112-Q117):

NEW QUESTION # 112
You have a network with ArubaOS-Switches for which Aruba ClearPass Policy Manager (CPPM) is acting as a TACACS+ server to authenticate managers. CPPM assigns the admins a TACACS+ privilege level, either manager or operator. You are now adding ArubaOS-CX switches to the network. ClearPass admins want to use the same CPPM service and policies to authenticate managers on the new switches.
What should you explain?

- A. This approach will work, but will need to be adjusted later if you want to assign managers to the default auditors group.
- B. This approach cannot work because the ArubaOS-CX switches do not accept standard TACACS+ privilege levels.
- C. This approach cannot work because the ArubaOS-CX switches do not support TACACS+.
- D. This approach will work to assign admins to the default "administrators" group, but not to the default "operators" group.

Answer: D

Explanation:
With ArubaOS-CX switches, the use of ClearPass Policy Manager (CPPM) as a TACACS+ server for authentication is supported. The privilege levels assigned by CPPM will translate onto the switches, where the "manager" privilege level typically maps to administrative capabilities and the "operator" privilege level maps to more limited capabilities. ArubaOS-CX does support standard TACACS+ privilege levels, so administrators can be assigned appropriately. If the ClearPass policies are correctly configured, they will work for both ArubaOS-Switches and ArubaOS-CX switches. The distinction between the "administrators" and "operators" groups is inherent in the ArubaOS-CX role-based access control, and these default groups need to be appropriately mapped to the TACACS+ privilege levels assigned by CPPM.

NEW QUESTION # 113
What is one difference between EAP-Tunneled Layer Security (EAP-TLS) and Protected EAP (PEAP)?

- A. EAP-TLS requires the supplicant to authenticate with a certificate, but PEAP allows the supplicant to use a username and password.
- B. EAP-TLS creates a TLS tunnel for transmitting user credentials, while PEAP authenticates the server and supplicant during a TLS handshake.
- C. EAP-TLS creates a TLS tunnel for transmitting user credentials securely, while PEAP protects user credentials with TKIP encryption.
- D. EAP-TLS begins with the establishment of a TLS tunnel, but PEAP does not use a TLS tunnel as part of its process.

Answer: A

Explanation:
EAP-TLS (Extensible Authentication Protocol - Transport Layer Security) and PEAP (Protected EAP) are two EAP methods used for 802.1X authentication in wireless networks, such as those configured with WPA3-Enterprise on HPE Aruba Networking solutions. Both methods are commonly used with ClearPass Policy Manager (CPPM) for secure authentication.
EAP-TLS:
Requires both the supplicant (client) and the server (e.g., CPPM) to present a valid certificate during authentication.
Establishes a TLS tunnel to secure the authentication process, but the primary authentication mechanism is the mutual certificate exchange. The client's certificate is used to authenticate the client, and the server's certificate authenticates the server.
PEAP:
Requires only the server to present a certificate to authenticate itself to the client.
Establishes a TLS tunnel to secure the authentication process, within which the client authenticates using a secondary method, typically a username and password (e.g., via MS-CHAPv2 or EAP-GTC).
Option A, "EAP-TLS begins with the establishment of a TLS tunnel, but PEAP does not use a TLS tunnel as part of its process," is incorrect. Both EAP-TLS and PEAP establish a TLS tunnel. In EAP-TLS, the TLS tunnel is used for the mutual certificate exchange, while in PEAP, the TLS tunnel protects the inner authentication (e.g., username/password).
Option B, "EAP-TLS requires the supplicant to authenticate with a certificate, but PEAP allows the supplicant to use a username and password," is correct. This is a key difference: EAP-TLS mandates certificate-based authentication for the client, while PEAP allows the client to authenticate with a username and password inside the TLS tunnel, making PEAP more flexible for environments where client certificates are not deployed.
Option C, "EAP-TLS creates a TLS tunnel for transmitting user credentials, while PEAP authenticates the server and supplicant during a TLS handshake," is incorrect. Both methods use a TLS tunnel, and both authenticate the server during the TLS handshake (using the server's certificate). In EAP-TLS, the client's certificate is also part of the TLS handshake, while in PEAP, the client's credentials (username/password) are sent inside the tunnel after the handshake.
Option D, "EAP-TLS creates a TLS tunnel for transmitting user credentials securely, while PEAP protects user credentials with TKIP encryption," is incorrect. PEAP does not use TKIP (Temporal Key Integrity Protocol) for protecting credentials; TKIP is a legacy encryption method used in WPA/WPA2 for wireless data encryption, not for EAP authentication. PEAP uses the TLS tunnel to protect the inner authentication credentials.
The HPE Aruba Networking ClearPass Policy Manager 6.11 User Guide states:
"EAP-TLS requires both the supplicant and the server to present a valid certificate for mutual authentication. The supplicant authenticates using its certificate, and the process is secured within a TLS tunnel. In contrast, PEAP requires only the server to present a certificate to establish a TLS tunnel, within which the supplicant can authenticate using a username and password (e.g., via MS-CHAPv2 or EAP-GTC). This makes PEAP more suitable for environments where client certificates are not deployed." (Page 292, EAP Methods Section) Additionally, the HPE Aruba Networking Wireless Security Guide notes:
"A key difference between EAP-TLS and PEAP is the client authentication method. EAP-TLS mandates that the client authenticate with a certificate, requiring certificate deployment on all clients. PEAP allows the client to authenticate with a username and password inside a TLS tunnel, making it easier to deploy in environments without client certificates." (Page 40, 802.1X Authentication Methods Section)
:

HPE Aruba Networking ClearPass Policy Manager 6.11 User Guide, EAP Methods Section, Page 292.
HPE Aruba Networking Wireless Security Guide, 802.1X Authentication Methods Section, Page 40.

NEW QUESTION # 114
What purpose does an initialization vector (IV) serve for encryption?

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

Answer: A

Explanation:
An initialization vector (IV) is a random or pseudo-random value used in encryption algorithms to enhance security. It is commonly used in symmetric encryption modes like Cipher Block Chaining (CBC) or Counter (CTR) modes with algorithms such as AES, which is used in WPA3 and other Aruba security features.
Option B, "It makes encryption algorithms more secure by ensuring that the same plaintext and key can produce different ciphertext," is correct. The primary purpose of an IV is to introduce randomness into the encryption process. When the same plaintext is encrypted with the same key multiple times, the IV ensures that the resulting ciphertext is different each time. This prevents attackers from identifying patterns in the ciphertext, which could otherwise be used to deduce the plaintext or key. For example, in AES-CBC mode, the IV is XORed with the first block of plaintext before encryption, and each subsequent block is chained with the previous ciphertext, ensuring unique outputs.
Option A, "It enables programs to convert easily-remembered passphrases to keys of a correct length," is incorrect. This describes a key derivation function (KDF), such as PBKDF2, which converts a passphrase into a cryptographic key of the correct length. An IV is not involved in key derivation.
Option C, "It helps parties to negotiate the keys and algorithms used to secure data before data transmission," is incorrect. This describes a key exchange or handshake protocol (e.g., Diffie-Hellman or the 4-way handshake in WPA3), not the role of an IV. The IV is used during the encryption process, not during key negotiation.
Option D, "It enables the conversion of asymmetric keys into keys that are suitable for symmetric encryption," is incorrect. This describes a process like hybrid encryption (e.g., using RSA to encrypt a symmetric key), which is not the purpose of an IV. An IV is used in symmetric encryption to enhance security, not to convert keys.
The HPE Aruba Networking Wireless Security Guide states:
"An initialization vector (IV) is a random value used in symmetric encryption algorithms like AES to enhance security. The IV ensures that the same plaintext encrypted with the same key produces different ciphertext each time, preventing attackers from identifying patterns in the ciphertext. In WPA3, for example, the IV is used in AES-GCMP encryption to ensure that each packet is encrypted uniquely, even if the same data is sent multiple times." (Page 28, Encryption Fundamentals Section) Additionally, the HPE Aruba Networking AOS-8 8.11 User Guide notes:
"The initialization vector (IV) in encryption algorithms like AES-CBC or AES-GCMP makes encryption more secure by ensuring that identical plaintext encrypted with the same key results in different ciphertext. This randomness prevents pattern analysis attacks, which could otherwise compromise the security of the encryption." (Page 282, Wireless Encryption Section)
:
HPE Aruba Networking Wireless Security Guide, Encryption Fundamentals Section, Page 28.
HPE Aruba Networking AOS-8 8.11 User Guide, Wireless Encryption Section, Page 282.

NEW QUESTION # 115
A company has an ArubaOS controller-based solution with a WPA3-Enterprise WLAN. which authenticates wireless clients to Aruba ClearPass Policy Manager (CPPM). The company has decided to use digital certificates for authentication A user's Windows domain computer has had certificates installed on it However, the Networks and Connections window shows that authentication has tailed for the user. The Mobility Controllers (MC's) RADIUS events show that it is receiving Access-Rejects for the authentication attempt.
What is one place that you can you look for deeper insight into why this authentication attempt is failing?

- A. the reports generated by Aruba ClearPass Insight
- B. the packets captured on the MC control plane destined to UDP 1812
- C. the Alerts tab in the authentication record in CPPM Access Tracker
- D. the RADIUS events within the CPPM Event Viewer

Answer: D

Explanation:
When an authentication attempt for a user's Windows domain computer is failing on a WPA3-Enterprise WLAN and the Mobility Controller is receiving Access-Rejects, one place to look for deeper insight is the RADIUS events within the CPPM Event Viewer. ClearPass Policy Manager (CPPM) logs all RADIUS authentication events, and the Event Viewer would show detailed information about why a particular authentication attempt was rejected. This could include reasons such as incorrect credentials, expired certificates, or policy mismatches. The CPPM Event Viewer is an essential troubleshooting tool within ClearPass to diagnose authentication issues, as indicated in the ClearPass Policy Manager documentation.

NEW QUESTION # 116
What is one of the roles of the network access server (NAS) in the AAA framewonx?

- A. It negotiates with each user's device to determine which EAP method is used for authentication
- B. It enforces access to network services and sends accounting information to the AAA server
- C. It authenticates legitimate users and uses policies to determine which resources each user is allowed to access.
- D. It determines which resources authenticated users are allowed to access and monitors each users session

Answer: B

Explanation:
In the AAA (Authentication, Authorization, and Accounting) framework, the role of the Network Access Server (NAS) is to act as a gateway that enforces access to network services and sends accounting information to the AAA server. The NAS initially requests authentication information from the user and then passes that information to the AAA server. It also enforces the access policies as provided by the AAA server after authentication and provides accounting data to the AAA server based on user activity.
:
Technical literature on AAA protocols which often includes a description of the roles and responsibilities of a Network Access Server.
Network security resources that discuss the NAS function within the AAA framework.

NEW QUESTION # 117
.....

By keeping minimizing weak points and maiming strong points, our HP HPE6-A78 exam materials are nearly perfect for you to choose. As a brand now, many companies strive to get our Aruba Certified Network Security Associate Exam HPE6-A78 practice materials to help their staffs achieve more certifications for our quality and accuracy.

Reliable Exam Sample

- Precise HPE6-A78 Sample Exam bring you First-Grade HPE6-A78 Reliable Test Vce for HP Aruba Certified Network Security Associate Exam □ Search on ▶ www.pdfvce.com ◀ for □ HPE6-A78 □ to obtain exam materials for free download □HPE6-A78 Testking
- Fantastic HPE6-A78 Sample Exam for Real Exam □ Search for 《 HPE6-A78 》 on □ www.prep4away.com □ immediately to obtain a free download □New HPE6-A78 Exam Cram
- myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, english.ashouweb.com, learn.vrccministries.com, xifeng.sbs, www.stes.tyc.edu.tw, motionentrance.edu.np, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, Disposable vapes

P.S. Free 2025 HP HPE6-A78 dumps are available on Google Drive shared by PassExamDumps: https://drive.google.com/open?id=1AhA1y5JoLipx-34XRCh-K1p_h73XM1Nr