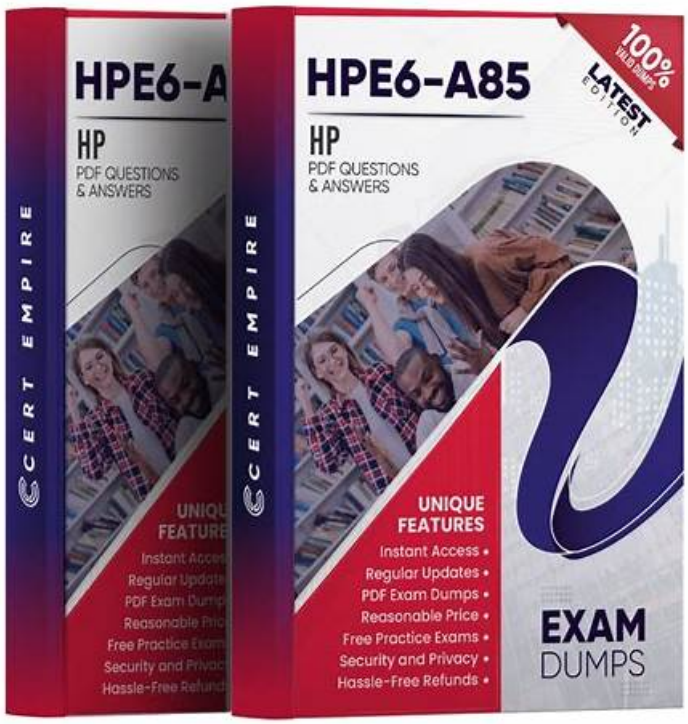
HPE6-A78 Download Fee | Valid HPE6-A78 Exam Discount



BTW, DOWNLOAD part of DumpsReview HPE6-A78 dumps from Cloud Storage: https://drive.google.com/open?id=1xtU6WMLfD3bwve5K6VFMH20W-gbyhWeI

Our users can prove to you that the hit rate of our HPE6-A78 exam questions is very high. And you can just see the data how many customers are visiting our HPE6-A78 study materials everyday. And the pass rate is also high as 98% to 100%. You can walk into the examination room with peace of mind, after which you will experience a very calm examination. As for the result, please come home and wait. Our HPE6-A78 training prep will not disappoint you.

HP HPE6-A78 exam is a certification exam designed for networking professionals who are interested in validating their knowledge and skills in network security. HPE6-A78 exam is specifically tailored for those who are looking to become Aruba Certified Network Security Associates. HPE6-A78 Exam is designed to test the candidate's understanding of Aruba's security solutions and their ability to implement them effectively.

>> HPE6-A78 Download Fee <<

Valid HPE6-A78 Exam Discount - HPE6-A78 New Exam Bootcamp

The successful outcomes are appreciable after you getting our HPE6-A78 exam prep. After buying our HPE6-A78 latest material, the change of gaining success will be over 98 percent. Many exam candidates ascribe their success to our HPE6-A78 real questions and become our regular customers eventually. Rather than blindly assiduous hardworking for amassing knowledge of computer, you can achieve success skillfully. They are masterpieces of experts who are willing to offer the most effective and accurate HPE6-A78 Latest Material for you.

HP HPE6-A78 (Aruba Certified Network Security Associate) Certification Exam is designed for IT professionals who are interested in demonstrating their expertise in network security. Aruba Certified Network Security Associate Exam certification exam is ideal for those who want to develop their skills in designing, implementing, and managing secure enterprise-level wireless networks. The HPE6-A78 Exam measures an individual's knowledge and abilities in wireless networking security protocols, technologies, and solutions.

HP Aruba Certified Network Security Associate Exam Sample Questions (Q130-Q135):

NEW QUESTION # 130
What distinguishes a Distributed Denial of Service (DDoS) attack from a traditional Denial or service attack (DoS)?

- A. A DDoS attack targets multiple devices, while a DoS Is designed to Incapacitate only one device
- B. A DDoS attack is launched from multiple devices, while a DoS attack is launched from a single device
- C. A DDoS attack originates from external devices, while a DoS attack originates from internal devices
- D. A DoS attack targets one server, a DDoS attack targets all the clients that use a server

Answer: C

NEW QUESTION # 131
What is a difference between radius and TACACS+?

- A. RADIUS uses Attribute Value Pairs (AVPs) in its messages, while TACACS+ does not use them.
- B. RADIUS combines the authentication and authorization process while TACACS+ separates them.
- C. RADIUS encrypts the complete packet, white TACACS+ only offers partial encryption.
- D. RADIUS uses TCP for Its connection protocol, while TACACS+ uses UDP tor its connection protocol.

Answer: B

NEW QUESTION # 132
You have enabled 802.1X authentication on an AOS-CX switch, including on port 1/1/1. That port has these port-access roles configured on it:
Fallback role = roleA
Auth role = roleB
Critical role = roleC
No other port-access roles are configured on the port. A client connects to that port. The user succeeds authentication, and CPPM does not send an Aruba-User-Role VSA.
What role does the client receive?

- A. The client receives roleB.
- B. The client receives roleC.
- C. The client receives roleA.
- D. The client is denied access.

Answer: A

Explanation:
In an AOS-CX switch environment, 802.1X authentication is used to authenticate clients connecting to ports, and roles are assigned based on the authentication outcome and configuration. The roles mentioned in the question-fallback, auth, and critical-have specific purposes in the AOS-CX port-access configuration:
Auth role (roleB): This role is applied when a client successfully authenticates via 802.1X and no specific role is assigned by the RADIUS server (e.g., via an Aruba-User-Role VSA). It is the default role for successful authentication.
Fallback role (roleA): This role is applied when no authentication method is attempted (e.g., the client does not support 802.1X or MAC authentication and no other method is configured).
Critical role (roleC): This role is applied when the switch cannot contact the RADIUS server (e.g., during a server timeout or failure), allowing the client to have limited access in a "critical" state.
In this scenario, the client successfully authenticates via 802.1X, and CPPM does not send an Aruba-User-Role VSA. Since authentication is successful, the switch applies the auth role (roleB) as the default role for successful authentication when no specific role is provided by the RADIUS server.
Option A, "The client receives roleC," is incorrect because the critical role is only applied when the RADIUS server is unreachable, which is not the case here since authentication succeeded.
Option B, "The client is denied access," is incorrect because the client successfully authenticated, so access is granted with the appropriate role.
Option D, "The client receives roleA," is incorrect because the fallback role is applied only when no authentication is attempted, not

when authentication succeeds.
The HPE Aruba Networking AOS-CX 10.12 Security Guide states:
"When a client successfully authenticates using 802.1X, the switch assigns the client to the auth role configured for the port, unless the RADIUS server specifies a different role via the Aruba-User-Role VSA. If no Aruba-User-Role VSA is present in the Access-Accept message, the auth role is applied." (Page 132, 802.1X Authentication Section) Additionally, the guide clarifies the roles:
"Auth role: Applied after successful 802.1X or MAC authentication if no role is specified by the RADIUS server."
"Fallback role: Applied when no authentication method is attempted."
"Critical role: Applied when the RADIUS server is unavailable." (Page 134, Port-Access Roles Section)
:
HPE Aruba Networking AOS-CX 10.12 Security Guide, 802.1X Authentication Section, Page 132.
HPE Aruba Networking AOS-CX 10.12 Security Guide, Port-Access Roles Section, Page 134.

NEW QUESTION # 133
You have configured a WLAN to use Enterprise security with the WPA3 version.
How does the WLAN handle encryption?

- A. Traffic is encrypted with AES and keys derived from a unique PMK per client.
- B. Traffic is encrypted with AES and keys derived from a PMK shared by all clients on the WLAN.
- C. Traffic is encrypted with TKIP and keys derived from a PMK shared by all clients on the WLAN.
- D. Traffic is encrypted with TKIP and keys derived from a unique PMK per client.

Answer: A

Explanation:
WPA3-Enterprise is a security protocol introduced to enhance the security of wireless networks, particularly in enterprise environments. It builds on the foundation of WPA2 but introduces stronger encryption and key management practices. In WPA3-Enterprise, authentication is typically performed using 802.1X, and encryption is handled using the Advanced Encryption Standard (AES).
WPA3-Enterprise Encryption: WPA3-Enterprise uses AES with the Galois/Counter Mode Protocol (GCMP) or Cipher Block Chaining Message Authentication Code Protocol (CCMP), both of which are AES-based encryption methods. WPA3 does not use TKIP (Temporal Key Integrity Protocol), which is a legacy encryption method used in WPA and early WPA2 deployments and is considered insecure.
Pairwise Master Key (PMK): In WPA3-Enterprise, the PMK is derived during the 802.1X authentication process (e.g., via EAP-TLS or EAP-TTLS). Each client authenticates individually with the authentication server (e.g., ClearPass), resulting in a unique PMK for each client. This PMK is then used to derive session keys (Pairwise Transient Keys, PTKs) for encrypting the client's traffic, ensuring that each client's traffic is encrypted with unique keys.
Option A, "Traffic is encrypted with TKIP and keys derived from a PMK shared by all clients on the WLAN," is incorrect because WPA3 does not use TKIP (it uses AES), and the PMK is not shared among clients in WPA3-Enterprise; each client has a unique PMK.
Option B, "Traffic is encrypted with TKIP and keys derived from a unique PMK per client," is incorrect because WPA3 does not use TKIP; it uses AES.
Option C, "Traffic is encrypted with AES and keys derived from a PMK shared by all clients on the WLAN," is incorrect because, in WPA3-Enterprise, the PMK is unique per client, not shared.
Option D, "Traffic is encrypted with AES and keys derived from a unique PMK per client," is correct. WPA3-Enterprise uses AES for encryption, and each client derives a unique PMK during 802.1X authentication, which is used to generate unique session keys for encryption.
The HPE Aruba Networking AOS-8 8.11 User Guide states:
"WPA3-Enterprise enhances security by using AES encryption with GCMP or CCMP. In WPA3-Enterprise mode, each client authenticates via 802.1X, resulting in a unique Pairwise Master Key (PMK) for each client. The PMK is used to derive session keys (Pairwise Transient Keys, PTKs) that encrypt the client's traffic with AES, ensuring that each client's traffic is protected with unique keys. WPA3 does not support TKIP, which is a legacy encryption method." (Page 285, WPA3-Enterprise Security Section)
Additionally, the HPE Aruba Networking Wireless Security Guide notes:
"WPA3-Enterprise requires 802.1X authentication, which generates a unique PMK for each client. This PMK is used to derive AES-based session keys, providing individualized encryption for each client's traffic and eliminating the risks associated with shared keys." (Page 32, WPA3 Security Features Section)
:
HPE Aruba Networking AOS-8 8.11 User Guide, WPA3-Enterprise Security Section, Page 285.
HPE Aruba Networking Wireless Security Guide, WPA3 Security Features Section, Page 32.

NEW QUESTION # 134
You are troubleshooting an authentication issue for Aruba switches that enforce 802 IX10 a cluster of Aruba ClearPass Policy Manager (CPPMs) You know that CPPM Is receiving and processing the authentication requests because the Aruba switches are showing Access-Rejects in their statistics However, you cannot find the record tor the Access-Rejects in CPPM Access Tracker What is something you can do to look for the records?

- A. Click Edit in Access viewer and make sure that the correct servers are selected.
- B. Verify that you are logged in to the CPPM Ul with read-write, not read-only, access
- C. Go to the CPPM Event Viewer, because this is where RADIUS Access Rejects are stored.
- D. Make sure that CPPM cluster settings are configured to show Access-Rejects

Answer: D

NEW QUESTION # 135
......