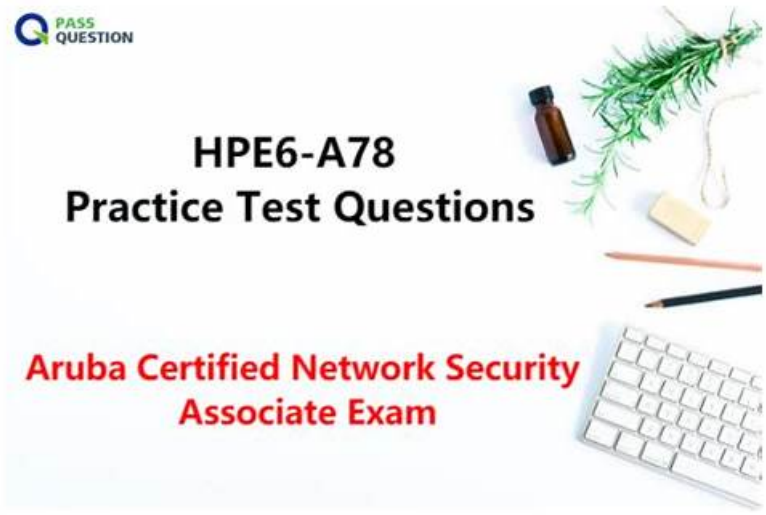
HPE6-A78 Reliable Exam Sample, Latest HPE6-A78 Exam Pass4sure



P.S. Free 2025 HP HPE6-A78 dumps are available on Google Drive shared by DumpStillValid: https://drive.google.com/open?id=1UkJKsW5wOOFhQ-CK55ImyGy7VU9OD__0

As far as our HPE6-A78 study guide is concerned, the PDF version brings you much convenience with regard to the following advantage. The PDF version of our HPE6-A78 learning materials contain demo where a part of questions selected from the entire version of our HPE6-A78 Exam Quiz is contained. In this way, you have a general understanding of our HPE6-A78 actual prep exam, which must be beneficial for your choice of your suitable exam files.

HPE6-A78 exam is designed for IT professionals who have experience in implementing network security solutions in enterprise environments. HPE6-A78 exam covers a wide range of topics, including network security fundamentals, wireless security, secure network access, and advanced firewall policies. Candidates who pass the HPE6-A78 Exam will have demonstrated their ability to implement and configure Aruba's network security solutions effectively.

>> HPE6-A78 Reliable Exam Sample <<

2025 High Pass-Rate HP HPE6-A78: Aruba Certified Network Security Associate Exam Reliable Exam Sample

DumpStillValid's HP HPE6-A78 Exam Training materials is virtually risk-free for you at the time of purchase. Before you buy, you can enter DumpStillValid website to download the free part of the exam questions and answers as a trial. So you can see the quality of the exam materials and we DumpStillValidis friendly web interface. We also offer a year of free updates. If you do not pass the exam, we will refund the full cost to you. We absolutely protect the interests of consumers. Training materials provided by DumpStillValid are very practical, and they are absolutely right for you. We can make you have a financial windfall.

HP Aruba Certified Network Security Associate Exam Sample Questions (Q12-Q17):

NEW QUESTION # 12
Refer to the exhibit.
Device A is establishing an HTTPS session with the Arubapedia web sue using Chrome. The Arubapedia web server sends the certificate shown in the exhibit What does the browser do as part of vacating the web server certificate?

- A. It uses the private key in the Arubapedia web site's certificate to check that certificate's signature
- B. It uses the private key in the DigiCert SHA2 Secure Server CA to check the certificate's signature.
- C. It uses the public key in the DigCert root CA certificate to check the certificate signature
- D. It uses the public key in the DigCen SHA2 Secure Server CA certificate to check the certificate's signature.

Answer: D

Explanation:
When a browser, like Chrome, is validating a web server's certificate, it uses the public key in the certificate's signing authority to verify the certificate's digital signature. In the case of the exhibit, the browser would use the public key in the DigiCert SHA2 Secure Server CA certificate to check the signature of the Arubapedia web server's certificate. This process ensures that the certificate was indeed issued by the claimed Certificate Authority (CA) and has not been tampered with.
:
Browser security documentation and SSL/TLS standards that explain the certificate validation process.
Cybersecurity educational resources that cover the principles of public key infrastructure (PKI) and certificate validation.

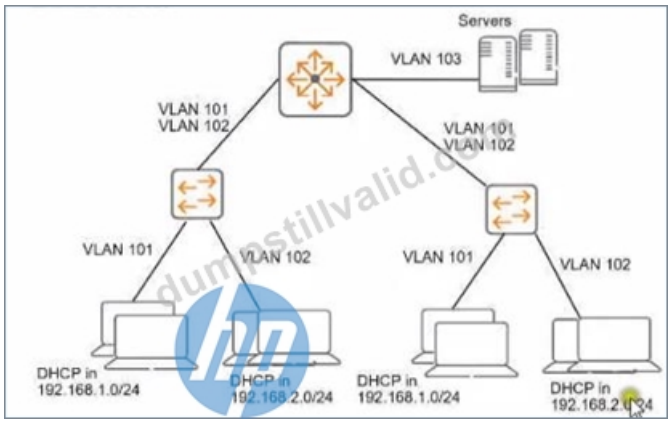
NEW QUESTION # 13
What is a use case for implementing RadSec instead of RADIUS?

- A. A university wants to protect communications between the students' devices and the network access server.
- B. A school district wants to protect messages sent between RADIUS clients and servers over an untrusted network.
- C. A corporation wants to implement EAP-TLS to authenticate wireless users at their main office.
- D. A organization wants to strengthen the encryption used to protect RADIUS communications without increasing complexity.

Answer: B

Explanation:
RadSec (RADIUS over TLS) is a protocol for transporting RADIUS messages over TLS-encrypted TCP/IP networks. The primary use case for implementing RadSec instead of traditional RADIUS is to protect RADIUS communications, particularly when those messages must travel across an untrusted network, such as the internet. RadSec provides confidentiality, integrity, and authentication for RADIUS traffic between clients and servers which may not be within a single secure network. In the case of a school district that wants to ensure the security of messages sent between RADIUS clients and servers over potentially insecure networks, RadSec would be the appropriate choice.

NEW QUESTION # 14
Refer to the exhibit.



You need to ensure that only management stations in subnet 192.168.1.0/24 can access the ArubaOS-Switches' CLI. Web Ul. and REST interfaces The company also wants to let managers use these stations to access other parts of the network What should you do?

- A. Specify 192.168.1.0.255.255.255.0 as authorized IP manager address
- B. Configure the switch to listen for these protocols on OOBM only.
- C. Establish a Control Plane Policing class that selects traffic from 192.168 1.0/24.
- D. Specify vlan 100 as the management vlan for the switches.

Answer: A

Explanation:
To ensure that only management stations in the subnet 192.168.1.0/24 can access the ArubaOS-Switches' Command Line Interface (CLI), Web UI, and REST interfaces, while also allowing managers to access other parts of the network, you should specify 192.168.1.0 255.255.255.0 as the authorized manager IP address on the switches. This configuration will restrict access to the

switch management interfaces to devices within the specified IP address range, effectively creating a management access list.
:
ArubaOS-Switch management and configuration guide detailing IP authorized manager settings.
Network management best practices which recommend controlling access to network devices' management interfaces.

NEW QUESTION # 15
What is a correct guideline for the management protocols that you should use on AOS-CX switches?

- A. Make sure that Telnet is disabled and use TFTP instead.
- B. Make sure that Telnet is disabled and use SSH instead.
- C. Make sure that HTTPS is disabled and use SSH instead.
- D. Make sure that SSH is disabled and use HTTPS instead.

Answer: B

Explanation:
AOS-CX switches support various management protocols for administrative access, such as SSH, Telnet, HTTPS, and TFTP. Security best practices for managing network devices, including AOS-CX switches, emphasize using secure protocols to protect management traffic from eavesdropping and unauthorized access.
Option B, "Make sure that Telnet is disabled and use SSH instead," is correct. Telnet is an insecure protocol because it sends all data, including credentials, in plaintext, making it vulnerable to eavesdropping. SSH (Secure Shell) provides encrypted communication for remote management, ensuring that credentials and commands are protected. HPE Aruba Networking recommends disabling Telnet and enabling SSH for secure management access on AOS-CX switches.
Option A, "Make sure that SSH is disabled and use HTTPS instead," is incorrect. SSH and HTTPS serve different purposes: SSH is for CLI access, while HTTPS is for web-based management. Disabling SSH would prevent secure CLI access, which is not a recommended practice. Both SSH and HTTPS should be enabled for secure management.
Option C, "Make sure that Telnet is disabled and use TFTP instead," is incorrect. TFTP (Trivial File Transfer Protocol) is used for file transfers (e.g., firmware updates), not for management access like Telnet or SSH. TFTP is also insecure (no encryption), so it's not a suitable replacement for Telnet.
Option D, "Make sure that HTTPS is disabled and use SSH instead," is incorrect. HTTPS is used for secure web-based management and should not be disabled. Both HTTPS and SSH are secure protocols and should be used together for different management interfaces (web and CLI, respectively).
The HPE Aruba Networking AOS-CX 10.12 Security Guide states:
"For secure management of AOS-CX switches, disable insecure protocols like Telnet, which sends data in plaintext, and use SSH instead. SSH provides encrypted communication for CLI access, protecting credentials and commands from eavesdropping. Use the command no telnet-server to disable Telnet and ssh-server to enable SSH. Additionally, enable HTTPS for web-based management with https-server to ensure all management traffic is encrypted." (Page 195, Secure Management Protocols Section)
Additionally, the HPE Aruba Networking Security Best Practices Guide notes:
"A key guideline for managing AOS-CX switches is to disable Telnet and enable SSH for CLI access. Telnet is insecure and should not be used in production environments, as it transmits credentials in plaintext. SSH ensures secure remote management, and HTTPS should also be enabled for web access." (Page 25, Management Security Section)
:
HPE Aruba Networking AOS-CX 10.12 Security Guide, Secure Management Protocols Section, Page 195.
HPE Aruba Networking Security Best Practices Guide, Management Security Section, Page 25.

NEW QUESTION # 16
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 PMK shared by all clients on the WLAN.
- B. Traffic is encrypted with TKIP and keys derived from a PMK shared by all clients on the WLAN.
- C. Traffic is encrypted with AES and keys derived from a unique PMK per client.
- D. Traffic is encrypted with TKIP and keys derived from a unique PMK per client.

Answer: C

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 # 17
.....

With the rapid development of society, people pay more and more attention to knowledge and skills. So every year a large number of people take HPE6-A78 tests to prove their abilities. But even the best people fail sometimes. In addition to the lack of effort, may also not make the right choice. A good choice can make one work twice the result with half the effort, and our HPE6-A78 Study Materials will be your right choice.

□HPE6-A78 Latest Training

- HPE6-A78 Actual Dump □ Valid HPE6-A78 Practice Materials □ HPE6-A78 Valid Test Pdf □ Search for （ HPE6-A78 ） on （ www.pdfvce.com ） immediately to obtain a free download □Real HPE6-A78 Exam Dumps
- Pass Guaranteed Quiz 2025 Newest HPE6-A78: Aruba Certified Network Security Associate Exam Reliable Exam Sample □ Go to website ➽ www.testkingpdf.com □ open and search for ➠ HPE6-A78 □ to download for free □Pdf HPE6-A78 Files
- Hot HPE6-A78 Reliable Exam Sample 100% Pass | Pass-Sure HPE6-A78: Aruba Certified Network Security Associate Exam 100% Pass □ Immediately open " www.pdfvce.com " and search for ➡ HPE6-A78 □□□ to obtain a free download □Reliable HPE6-A78 Practice Questions
- Why Do You Need to Trust HP HPE6-A78 Exam Questions? □ Open website ✔ www.testkingpdf.com □✔□ and search for ▸ HPE6-A78 ◂ for free download □HPE6-A78 Latest Braindumps Book
- www.stes.tyc.edu.tw, www.acolsi.org, shortcourses.russellcollege.edu.au, lms.slikunedu.in, m.871v.com, www.stes.tyc.edu.tw, billfor6581.bluxeblog.com, www.stes.tyc.edu.tw, daotao.wisebusiness.edu.vn, 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

BONUS!!! Download part of DumpStillValid HPE6-A78 dumps for free: https://drive.google.com/open?id=1UkJKsW5wOOFhQ-CK55ImyGy7VU9OD__0