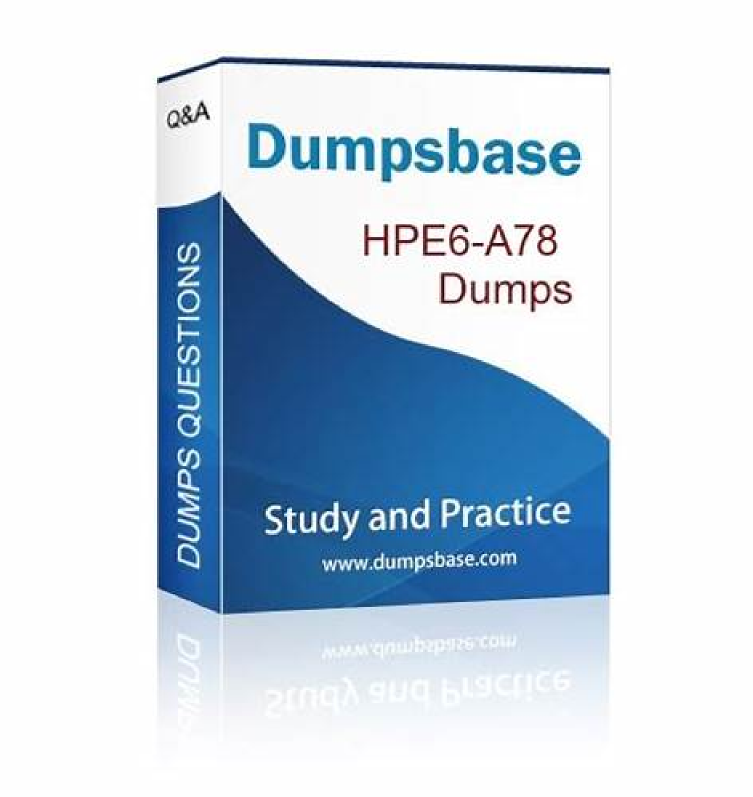
HPE6-A78 Test Dump, HPE6-A78 Latest Test Labs



DOWNLOAD the newest Pass4guide HPE6-A78 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1gdPNdxnZsnXqTii3b3lBoQNY-zHZRIBc

First and foremost, the pass rate of our HPE6-A78 training guide among our customers has reached as high as 98% to 100%, which marks the highest pass rate in the field, we are waiting for you to be the next beneficiary. Second, you can get our HPE6-A78 practice test only in 5 to 10 minutes after payment, which enables you to devote yourself to study with our HPE6-A78 Exam Questions as soon as possible. Last but not least, you will get the privilege to enjoy free renewal of our HPE6-A78 preparation materials during the whole year. All of the staffs in our company wish you early success.

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 Test Dump <<

HPE6-A78 Latest Test Labs, Reliable HPE6-A78 Source

The price of Pass4guide HP HPE6-A78 updated exam dumps is affordable. You can try the free demo version of any HP HPE6-A78 exam dumps format before buying. For your satisfaction, Pass4guide gives you a free demo download facility. You can test the features and then place an order. So, these real and updated Aruba Certified Network Security Associate Exam (HPE6-A78) dumps are essential to pass the HPE6-A78 exam on the first try.

HPE6-A78 exam covers a wide range of topics, including Aruba security technologies, firewall policies, VPN technologies, and network security best practices. Candidates who Pass HPE6-A78 Exam will have a deep understanding of Aruba's security architecture and be able to implement and manage security solutions that protect networks from various threats and attacks. Aruba Certified Network Security Associate Exam certification can help professionals advance their careers and prove their ability to design, implement and manage effective security solutions in complex network environments.

HP Aruba Certified Network Security Associate Exam Sample Questions (Q164-Q169):

NEW QUESTION # 164

A company has HPE Aruba Networking Mobility Controllers (MCs), HPE Aruba Networking campus APs, and AOS-CX switches. The company plans to use HPE Aruba Networking ClearPass Policy Manager (CPPM) to classify endpoints by type. The company is contemplating the use of ClearPass's TCP fingerprinting capabilities.
What is a consideration for using those capabilities?

- A. You will need to mirror traffic to one of CPPM's span ports from a device such as a core routing switch.
- B. AOS-CX switches do not offer the support necessary for CPPM to use TCP fingerprinting on wired endpoints.
- C. TCP fingerprinting of wireless endpoints requires a third-party Mobility Device Management (MDM) solution.
- D. ClearPass admins will need to provide the credentials of an API admin account to configure on HPE Aruba Networking devices.

Answer: A

Explanation:
HPE Aruba Networking ClearPass Policy Manager (CPPM) uses TCP fingerprinting as a passive profiling method to classify endpoints by analyzing TCP packet headers (e.g., TTL, window size) to identify the operating system (e.g., Windows, Linux). The company in this scenario has Mobility Controllers (MCs), campus APs, and AOS-CX switches, and wants to use CPPM's TCP fingerprinting capabilities for endpoint classification.
TCP Fingerprinting: This method requires CPPM to receive TCP traffic from endpoints. Since CPPM is not typically inline with network traffic, the traffic must be mirrored to CPPM for analysis. This is often done using a SPAN (Switched Port Analyzer) port or mirror port on a switch or controller.
Option A, "You will need to mirror traffic to one of CPPM's span ports from a device such as a core routing switch," is correct. For CPPM to perform TCP fingerprinting, it needs to see the TCP traffic from endpoints. This is typically achieved by mirroring traffic from a core routing switch (or another device like an MC) to a SPAN port on the CPPM server. For example, on an AOS-CX switch, you can configure a mirror session with the command mirror session 1 destination interface <CPPM-port> source vlan <vlan-id> to send traffic to CPPM. This is a key consideration for enabling TCP fingerprinting.
Option B, "ClearPass admins will need to provide the credentials of an API admin account to configure on HPE Aruba Networking devices," is incorrect. TCP fingerprinting does not require API credentials. It is a passive profiling method that analyzes mirrored traffic, and no API interaction is needed between CPPM and Aruba devices for this purpose.
Option C, "AOS-CX switches do not offer the support necessary for CPPM to use TCP fingerprinting on wired endpoints," is incorrect. AOS-CX switches support mirroring traffic to CPPM (e.g., using a mirror session), which enables CPPM to perform TCP fingerprinting on wired endpoints. The switch does not need to perform the fingerprinting itself; it only needs to send the traffic to CPPM.
Option D, "TCP fingerprinting of wireless endpoints requires a third-party Mobility Device Management (MDM) solution," is incorrect. TCP fingerprinting is a built-in capability of CPPM and does not require an MDM solution. For wireless endpoints, the MC can mirror client traffic to CPPM (e.g., using a datapath mirror), allowing CPPM to perform TCP fingerprinting.
The HPE Aruba Networking ClearPass Policy Manager 6.11 User Guide states:
"TCP fingerprinting requires ClearPass to receive TCP traffic from endpoints for analysis. A key consideration is that you must mirror traffic to one of ClearPass's SPAN ports from a device such as a core routing switch or Mobility Controller. For example, on an AOS-CX switch, configure a mirror session with mirror session 1 destination interface <CPPM-port> source vlan <vlan-id> to send traffic to ClearPass for TCP fingerprinting." (Page 248, TCP Fingerprinting Section) Additionally, the HPE Aruba Networking AOS-8 8.11 User Guide notes:
"For ClearPass to perform TCP fingerprinting on wireless endpoints, the Mobility Controller can mirror client traffic to ClearPass using a datapath mirror. For wired endpoints, an AOS-CX switch can mirror traffic to ClearPass's SPAN port, enabling TCP fingerprinting without requiring additional support on the switch itself." (Page 351, Device Profiling with CPPM Section)
:
HPE Aruba Networking ClearPass Policy Manager 6.11 User Guide, TCP Fingerprinting Section, Page 248.
HPE Aruba Networking AOS-8 8.11 User Guide, Device Profiling with CPPM Section, Page 351.

NEW QUESTION # 165

Your company policies require you to encrypt logs between network infrastructure devices and Syslog servers. What should you do to meet these requirements on an ArubaOS-CX switch?

- A. Specify a priv key with the Syslog settings that matches a priv key on the Syslog server.
- B. Set up RadSec and then enable Syslog as a protocol carried by the RadSec tunnel.

- C. Specify the Syslog server with the UDP option and then add an CPsec tunnel that selects Syslog.
- D. Specify the Syslog server with the TLS option and make sure the switch has a valid certificate.

Answer: D

Explanation:
To ensure secure transmission of log data over the network, particularly when dealing with sensitive or critical information, using TLS (Transport Layer Security) for encrypted communication between network devices and syslog servers is necessary:
Secure Logging Setup: When configuring an ArubaOS-CX switch to send logs securely to a Syslog server, specifying the server with the TLS option ensures that all transmitted log data is encrypted.
Additionally, the switch must have a valid certificate to establish a trusted connection, preventing potential eavesdropping or tampering with the logs in transit.
Other Options:
Option B, Option C, and Option D are less accurate or applicable for directly encrypting log data between the device and Syslog server as specified in the company policies.

NEW QUESTION # 166
You are checking the Security Dashboard in the Web UI for your AOS solution and see that Wireless Intrusion Prevention (WIP) has discovered a rogue radio operating in ad hoc mode with open security. What correctly describes a threat that the radio could pose?

- A. It could open a backdoor into the corporate LAN for unauthorized users.
- B. It could be attempting to conceal itself from detection by changing its BSSID and SSID frequently.
- C. It is flooding the air with many wireless frames in a likely attempt at a DoS attack.
- D. It is running in a non-standard 802.11 mode and could effectively jam the wireless signal.

Answer: A

Explanation:
The AOS Security Dashboard in an AOS-8 solution (Mobility Controllers or Mobility Master) provides visibility into wireless threats detected by the Wireless Intrusion Prevention (WIP) system. The scenario describes a rogue radio operating in ad hoc mode with open security. Ad hoc mode in 802.11 allows devices to communicate directly with each other without an access point (AP), forming a peer-to-peer network. Open security means no encryption or authentication is required to connect.
Ad Hoc Mode Threat: An ad hoc network created by a rogue device can pose significant risks, especially if a corporate client connects to it. Since ad hoc mode allows direct device-to-device communication, a client that joins the ad hoc network might inadvertently bridge the corporate LAN to the rogue network, especially if the client is also connected to the corporate network (e.g., via a wired connection or another wireless interface).
Option B, "It could open a backdoor into the corporate LAN for unauthorized users," is correct. If a corporate client connects to the rogue ad hoc network (e.g., due to a misconfiguration or auto-connect setting), the client might bridge the ad hoc network to the corporate LAN, allowing unauthorized users on the ad hoc network to access corporate resources. This is a common threat with ad hoc networks, as they bypass the security controls of the corporate AP infrastructure.
Option A, "It could be attempting to conceal itself from detection by changing its BSSID and SSID frequently," is incorrect. While changing BSSID and SSID can be a tactic to evade detection, this is not a typical characteristic of ad hoc networks and is not implied by the scenario. Ad hoc networks are generally visible to WIP unless explicitly hidden.
Option C, "It is running in a non-standard 802.11 mode and could effectively jam the wireless signal," is incorrect. Ad hoc mode is a standard 802.11 mode, not a non-standard one. While a rogue device could potentially jam the wireless signal, this is not a direct threat posed by ad hoc mode with open security.
Option D, "It is flooding the air with many wireless frames in a likely attempt at a DoS attack," is incorrect. There is no indication in the scenario that the rogue radio is flooding the air with frames. While ad hoc networks can be used in DoS attacks, the primary threat in this context is the potential for unauthorized access to the corporate LAN.
The HPE Aruba Networking AOS-8 8.11 User Guide states:
"A rogue radio operating in ad hoc mode with open security poses a significant threat, as it can open a backdoor into the corporate LAN. If a corporate client connects to the ad hoc network, it may bridge the ad hoc network to the corporate LAN, allowing unauthorized users to access corporate resources. This is particularly dangerous if the client is also connected to the corporate network via another interface." (Page 422, Wireless Threats Section) Additionally, the HPE Aruba Networking Security Guide notes:
"Ad hoc networks detected by WIP are a concern because they can act as a backdoor into the corporate LAN. A client that joins an ad hoc network with open security may inadvertently allow unauthorized users to access the corporate network, bypassing the security controls of authorized APs." (Page 73, Ad Hoc Network Threats Section)
:

HPE Aruba Networking AOS-8 8.11 User Guide, Wireless Threats Section, Page 422.
HPE Aruba Networking Security Guide, Ad Hoc Network Threats Section, Page 73.

NEW QUESTION # 167
How does the AOS firewall determine which rules to apply to a specific client's traffic?

- A. The firewall applies the rules in policies associated with the client's user role.
- B. The firewall applies the rules in policies associated with the client's WLAN.
- C. The firewall applies every rule that includes the client's IP address as the source or destination.
- D. The firewall applies every rule that includes the client's IP address as the source.

Answer: A

Explanation:
In an AOS-8 architecture, the Mobility Controller (MC) includes a stateful firewall that enforces policies on client traffic. The firewall uses user roles to apply policies, allowing granular control over traffic based on the client's identity and context.
User Roles: In AOS-8, each client is assigned a user role after authentication (e.g., via 802.1X, MAC authentication, or captive portal). The user role contains firewall policies (rules) that define what traffic is allowed or denied for clients in that role. For example, a "guest" role might allow only HTTP/HTTPS traffic, while an "employee" role might allow broader access.
Option A, "The firewall applies the rules in policies associated with the client's user role," is correct. The AOS firewall evaluates traffic based on the user role assigned to the client. Each role has a set of policies (rules) that are applied in order, and the first matching rule determines the action (permit or deny). For example, if a client is in the "employee" role, the firewall applies the rules defined in the "employee" role's policy.
Option B, "The firewall applies every rule that includes the client's IP address as the source," is incorrect. The firewall does not apply rules based solely on the client's IP address; it uses the user role. Rules within a role may include IP addresses, but the role determines which rules are evaluated.
Option C, "The firewall applies the rules in policies associated with the client's WLAN," is incorrect. While the WLAN configuration defines the initial role for clients (e.g., the default 802.1X role), the firewall applies rules based on the client's current user role, which may change after authentication (e.g., via a RADIUS VSA like Aruba-User-Role).
Option D, "The firewall applies every rule that includes the client's IP address as the source or destination," is incorrect for the same reason as Option B. The firewall uses the user role to determine which rules to apply, not just the client's IP address.
The HPE Aruba Networking AOS-8 8.11 User Guide states:
"The AOS firewall on the Mobility Controller applies rules based on the user role assigned to a client. Each user role contains a set of firewall policies that define the allowed or denied traffic for clients in that role. For example, a policy in the 'employee' role might include a rule like ipv4 user any http permit to allow HTTP traffic. The firewall evaluates the rules in the client's role in order, and the first matching rule determines the action for the traffic." (Page 325, Firewall Policies Section) Additionally, the HPE Aruba Networking Security Guide notes:
"User roles in AOS-8 provide a powerful mechanism for firewall policy enforcement. The firewall determines which rules to apply to a client's traffic by looking at the policies associated with the client's user role, which is assigned during authentication or via a RADIUS VSA like Aruba-User-Role." (Page 50, Role-Based Access Control Section)
:
HPE Aruba Networking AOS-8 8.11 User Guide, Firewall Policies Section, Page 325.
HPE Aruba Networking Security Guide, Role-Based Access Control Section, Page 50.

NEW QUESTION # 168
What is a reason to set up a packet capture on an Aruba Mobility Controller (MC)?

- A. You want the MC to analyze wireless clients' traffic at a lower level, so that the ArubaOS firewall can control the traffic I based on application.
- B. The company wants to use ClearPass Policy Manager (CPPM) to profile devices and needs to receive HTTP User-Agent strings from the MC.
- C. You want the MC to analyze wireless clients' traffic at a lower level, so that the ArubaOS firewall can control Web traffic based on the destination URL.
- D. The security team believes that a wireless endpoint connected to the MC is launching an attack and wants to examine the traffic more closely.

Answer: D

Explanation:

Setting up a packet capture on an Aruba Mobility Controller (MC) is particularly useful in scenarios where detailed analysis of network traffic is necessary to identify and address security concerns. Option B is the correct answer because it directly addresses the need to closely examine the traffic of a potentially malicious wireless endpoint. Packet capture on the MC allows the security team to collect and analyze traffic to/from specific endpoints in real-time, providing valuable insights into the nature of the traffic and potentially identifying harmful activities. This capability is essential for forensics and troubleshooting security incidents, enabling administrators to respond effectively to threats.
References:
Aruba Mobility Controller Configuration Guide
Aruba Networks Official Documentation

NEW QUESTION # 169
......

HPE6-A78 Latest Test Labs: https://www.pass4guide.com/HPE6-A78-exam-guide-torrent.html

- Exam HPE6-A78 Simulator □ HPE6-A78 Frenquent Update □ New HPE6-A78 Exam Dumps □ Open ➥ www.pass4test.com □ enter □ HPE6-A78 □ and obtain a free download □Valid HPE6-A78 Practice Materials
- Buy HP HPE6-A78 Pdfvce Exam Questions Today Save Time and Money □ Easily obtain free download of 「HPE6-A78」 by searching on [www.pdfvce.com] □Updated HPE6-A78 CBT
- Valid HPE6-A78 Exam Bootcamp ℹ HPE6-A78 Exam Dumps Free □ Download HPE6-A78 Demo □ Download □ HPE6-A78 □ for free by simply entering ✔ www.testkingpass.com □✔□ website ↕HPE6-A78 New Exam Bootcamp
- Authentic HP HPE6-A78 Exam Questions □ Open website □ www.pdfvce.com □ and search for ➽ HPE6-A78 □ for free download □Download HPE6-A78 Demo
- Buy HP HPE6-A78 www.troytecdumps.com Exam Questions Today Save Time and Money □ Easily obtain ➽ HPE6-A78 □ for free download through ▷ www.troytecdumps.com ◁ □HPE6-A78 Intereactive Testing Engine
- HPE6-A78 latest exam question - HPE6-A78 training guide dumps - HPE6-A78 valid study torrent □ Enter ▶ www.pdfvce.com ◀ and search for ➥ HPE6-A78 □ to download for free □Exam HPE6-A78 Simulator
- HPE6-A78 Braindumps □ New HPE6-A78 Exam Dumps □ Valid HPE6-A78 Exam Bootcamp □ Open 【 www.troytecdumps.com 】 and search for ⇛ HPE6-A78 ⇚ to download exam materials for free □Latest HPE6-A78 Mock Test
- Download HPE6-A78 Demo □ HPE6-A78 Valid Exam Experience □ Exam HPE6-A78 Simulator □ Copy URL ➠ www.pdfvce.com □ open and search for 「HPE6-A78」 to download for free □Certification HPE6-A78 Test Answers
- HPE6-A78 Latest Exam Tips □ Latest HPE6-A78 Mock Test □ Latest HPE6-A78 Mock Test □ Open ➡ www.pdfdumps.com □□□ enter 「HPE6-A78」 and obtain a free download □HPE6-A78 Practice Test
- HPE6-A78 Braindumps □ Updated HPE6-A78 CBT □ HPE6-A78 Frenquent Update □ Search on ➡ www.pdfvce.com □□□ for { HPE6-A78 } to obtain exam materials for free download □HPE6-A78 Frenquent Update
- Fast and Effective Preparation With HPE6-A78 Aruba Certified Network Security Associate Exam Exam Questions □ Go to website □ www.prep4sures.top □ open and search for □ HPE6-A78 □ to download for free □Practice HPE6-A78 Exam Online
- 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, 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, motionentrance.edu.np, seostationaoyon.com, www.stes.tyc.edu.tw, 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, kemono.im, www.stes.tyc.edu.tw, Disposable vapes

BTW, DOWNLOAD part of Pass4guide HPE6-A78 dumps from Cloud Storage: https://drive.google.com/open?id=1gdPNdxnZsnXqTii3b3lBoQNY-zHZRIBc