HP ACNSA HPE6-A78 Practice Questions

Shared by Michael on 17-08-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Refer to the exhibit, which shows the settings on the company's MCs.

--- Mobility Controller

Dashboard General Admin AirWave CPSec Certificates

Configuration

WLANs v Control Plane Security

Roles & Policies Enable CP Sec

Access Points Enable auto cert provisioning:

You have deployed about 100 new Aruba 335-APs. What is required for the APs to become managed?

Options:

A- installing CA-signed certificates on the APs
B- installing self-signed certificates on the APs
C- approving the APs as authorized APs on the AP whitelist
D- configuring a PAPI key that matches on the APs and MCs

Answer:

C

Explanation:

Based on the exhibit, which shows the settings on the company's Mobility Controllers (MCs), with 'Control Plane Security' enabled and 'Enable auto cert provisioning' available, new Aruba 335-APs require approval on the MC to become managed. This is commonly done by adding the APs to an authorized AP whitelist, after which they can be automatically provisioned with certificates generated by the MC.

Question 2

Question Type: MultipleChoice

You have an Aruba solution with multiple Mobility Controllers (MCs) and campus APs. You want to deploy a WPA3-Enterprise WLAN and authenticate users to Aruba ClearPass Policy Manager (CPPM) with EAP-TLS.

What is a guideline for ensuring a successful deployment?

Options:

A- Avoid enabling CNSA mode on the WLAN, which requires the internal MC RADIUS server.
B- Ensure that clients trust the root CA for the MCs' Server Certificates.
C- Educate users in selecting strong passwords with at least 8 characters.
D- Deploy certificates to clients, signed by a CA that CPPM trusts.

Answer:

D

Explanation:

For WPA3-Enterprise with EAP-TLS, it's crucial that clients have a trusted certificate installed for the authentication process. EAP-TLS relies on a mutual exchange of certificates for authentication. Deploying client certificates signed by a CA that CPPM trusts ensures that the ClearPass Policy Manager can verify the authenticity of the client certificates during the TLS handshake process. Trust in the root CA is typically required for the server side of the authentication process, not the client side, which is covered by the client's own certificate.

Question 3

Question Type: MultipleChoice

A company is deploying ArubaOS-CX switches to support 135 employees, which will tunnel client traffic to an Aruba Mobility Controller (MC) for the MC to apply firewall policies and deep packet inspection (DPI). This MC will be dedicated to receiving traffic from the ArubaOS-CX switches.

What are the licensing requirements for the MC?

Options:

A- one AP license per-switch

B- one PEF license per-switch
C- one PEF license per-switch. and one WCC license per-switch
D- one AP license per-switch. and one PEF license per-switch

Answer:

B

Explanation:

When deploying ArubaOS-CX switches that tunnel client traffic to an Aruba Mobility Controller (MC), the licensing requirements typically involve Policy Enforcement Firewall (PEF) licenses. These licenses enable the MC to enforce firewall policies and perform deep packet inspection (DPI). Therefore, for each switch tunneling traffic to the MC, a PEF license would be necessary.

Question 4

Question Type: MultipleChoice

You are deploying an Aruba Mobility Controller (MC). What is a best practice for setting up secure management access to the ArubaOS Web UP

Options:

A- Avoid using external manager authentication tor the Web UI.
B- Change the default 4343 port tor the web UI to TCP 443.
C- Install a CA-signed certificate to use for the Web UI server certificate.
D- Make sure to enable HTTPS for the Web UI and select the self-signed certificate Installed in the factory.

Answer:

C

Explanation:

For securing management access to the ArubaOS Web UI of an Aruba Mobility Controller (MC), it is a best practice to install a certificate signed by a Certificate Authority (CA). This ensures that communications between administrators and the MC are secured with trusted encryption, which greatly reduces the risk of man-in-the-middle attacks. Using a CA-signed certificate enhances the trustworthiness of the connection over self-signed certificates, which do not offer

the same level of assurance. :

ArubaOS documentation on management access security.

Question 5

Question Type: MultipleChoice

You have been instructed to look in an AOS Security Dashboard's client list. Your goal is to find clients that belong to the company and have connected to devices that might belong to hackers.

Which client fits this description?

Options:

A- MAC address: d8:50:e6:f3:6d:a4; Client Classification: Authorized; AP Classification: Suspected Rogue
B- MAC address: d8:50:e6:f3:6e:c5; Client Classification: Interfering; AP Classification: Neighbor
C- MAC address: d8:50:e6:f3:6e:60; Client Classification: Interfering; AP Classification: Interfering
D- MAC address: d8:50:e6:f3:70:ab; Client Classification: Interfering; AP Classification: Suspected Rogue

Answer:

A

Explanation:

The AOS Security Dashboard in an AOS-8 solution (Mobility Controllers or Mobility Master) provides a client list through its Wireless Intrusion Prevention (WIP) system, showing the classification of clients and the APs they are connected to. The goal is to identify clients that belong to the company (Authorized clients) and have connected to devices that might belong to hackers (rogue or suspected rogue APs).

Client Classification:

Authorized: A client that has successfully authenticated to an authorized AP and is part of the company's network (e.g., an employee device).

Interfering: A client that is not authenticated to the company's network and is considered external or potentially malicious.

AP Classification:

Authorized: An AP that is part of the company's network and managed by the MC.

Suspected Rogue: An AP that is not authorized and is suspected of being malicious, often because it exhibits suspicious behavior (e.g., a BSSID close to an authorized AP, indicating potential spoofing).

Neighbor: An AP that is not part of the company's network but is not connected to the wired network (e.g., a nearby AP from another organization).

Interfering: An AP that is not part of the company's network and may be causing interference, but is not necessarily malicious.

The requirement is to find a client that is Authorized (belongs to the company) and connected to a Suspected Rogue AP (might belong to hackers).

Option A: MAC address: d8:50:e6:f3:6d:a4; Client Classification: Authorized; AP Classification: Suspected Rogue

This client is classified as 'Authorized,' meaning it belongs to the company, and it is connected to a 'Suspected Rogue' AP, which might belong to hackers. This matches the requirement perfectly.

Option B: MAC address: d8:50:e6:f3:6e:c5; Client Classification: Interfering; AP Classification: Neighbor

This client is 'Interfering' (not a company client) and connected to a 'Neighbor' AP, which is not considered a hacker's device (it's just a nearby AP).

Option C: MAC address: d8:50:e6:f3:6e:60; Client Classification: Interfering; AP Classification: Interfering

This client is 'Interfering' (not a company client) and connected to an 'Interfering' AP, which is not necessarily a hacker's device (it may just be causing interference).

Option D: MAC address: d8:50:e6:f3:70:ab; Client Classification: Interfering; AP Classification: Suspected Rogue

This client is 'Interfering' (not a company client), although it is connected to a 'Suspected Rogue' AP. It does not meet the requirement of being a company client.

The HPE Aruba Networking AOS-8 8.11 User Guide states:

'The Security Dashboard's client list in ArubaOS shows the classification of each client and the AP it is connected to. An 'Authorized' client is one that has successfully authenticated to an authorized AP and is part of the company's network. A 'Suspected Rogue' AP is an unauthorized AP that exhibits suspicious behavior, such as a BSSID close to an authorized AP, indicating potential spoofing by a hacker. To identify security risks, look for authorized clients connected to suspected rogue APs, as this may indicate a company device has connected to a malicious AP.' (Page 415, Security Dashboard Section)

Additionally, the HPE Aruba Networking Security Guide notes:

'WIP classifies clients as 'Authorized' if they have authenticated to an authorized AP managed by the controller. A 'Suspected Rogue' AP is a potential threat, as it may be attempting to mimic a legitimate AP to lure clients. Identifying authorized clients connected to suspected rogue APs is critical for detecting potential attacks, such as man-in-the-middle attempts by hackers.' (Page 78, WIP Classifications Section)

:

HPE Aruba Networking AOS-8 8.11 User Guide, Security Dashboard Section, Page 415.

HPE Aruba Networking Security Guide, WIP Classifications Section, Page 78.

==========

Question 6

Question Type: MultipleChoice

What is one of the roles of the network access server (NAS) in the AAA framework?

Options:

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

Answer:

C

Explanation:

The AAA (Authentication, Authorization, and Accounting) framework is used in network security to manage user access. In this framework, the Network Access Server (NAS) plays a specific role. In an HPE Aruba Networking environment, the NAS is typically a device like a Mobility Controller (MC) or an AOS-CX switch that interacts with an AAA server (e.g., ClearPass Policy Manager, CPPM) to authenticate users.

NAS Role in AAA:

Authentication: The NAS acts as a client to the AAA server (e.g., via RADIUS), forwarding authentication requests from the user's device to the server. It does not perform the authentication itself; the AAA server authenticates the user.

Authorization: After authentication, the NAS receives authorization attributes from the AAA server (e.g., a user role via Aruba-User-Role VSA) and enforces access policies (e.g., firewall rules, VLAN assignment) based on those attributes.

Accounting: The NAS sends accounting information (e.g., session start/stop, data usage) to the AAA server to track user activity.

Option A, 'It negotiates with each user's device to determine which EAP method is used for authentication,' is incorrect. The NAS does not negotiate the EAP method with the user's device. The EAP method (e.g., EAP-TLS, PEAP) is determined by the configuration on the NAS and the AAA server, and the client must support the configured method. The negotiation of EAP methods occurs between the client (supplicant) and the AAA server, with the NAS acting as a pass-through.

Option B, 'It determines which resources authenticated users are allowed to access and monitors each user's session,' is incorrect. The NAS enforces access policies based on authorization attributes received from the AAA server, but it does not determine which resources users can access---that decision is made by the AAA server based on its policies. Monitoring sessions is part of accounting, but this option overstates the NAS's role in determining access.

Option C, 'It enforces access to network services and sends accounting information to the AAA server,' is correct. The NAS enforces access by applying policies (e.g., firewall rules, VLANs) based on the authorization attributes received from the AAA server. It also sends accounting information (e.g., session start/stop, data usage) to the AAA server to track user activity, fulfilling its role in the accounting part of AAA.

Option D, 'It authenticates legitimate users and uses policies to determine which resources each user is allowed to access,' is incorrect. The NAS does not authenticate users; the AAA server performs authentication. The NAS also does not determine resource access; it enforces the policies provided by the AAA server.

The HPE Aruba Networking AOS-8 8.11 User Guide states:

'In the AAA framework, the Network Access Server (NAS), such as a Mobility Controller, acts as a client to the AAA server (e.g., a RADIUS server). The NAS forwards authentication requests from the user's device to the AAA server, enforces access to network services based on the authorization attributes returned by the server (e.g., user role, VLAN), and sends accounting information, such as session start and stop records, to the AAA server for tracking.' (Page 310, AAA Framework Section)

Additionally, the HPE Aruba Networking ClearPass Policy Manager 6.11 User Guide notes:

'The NAS in the AAA framework, such as an Aruba Mobility Controller, does not authenticate users itself; it forwards authentication requests to the AAA server (ClearPass). After authentication, the NAS enforces access policies based on the server's response and sends accounting data to the AAA server to log user activity, such as session duration and data usage.' (Page 280, NAS Role in AAA Section)

:

HPE Aruba Networking AOS-8 8.11 User Guide, AAA Framework Section, Page 310.

HPE Aruba Networking ClearPass Policy Manager 6.11 User Guide, NAS Role in AAA Section, Page 280.

==========

Question 7

Question Type: MultipleChoice

Which is a use case for enabling Control Plane Policing on Aruba switches?

Options:

A- to prevent unauthorized network devices from sending routing updates
B- to prevent the switch from accepting routing updates from unauthorized users
C- to encrypt traffic between tunneled node switches and Mobility Controllers (MCs)
D- to mitigate Denial of Service (Dos) attacks on the switch

Answer:

D

Explanation:

Control Plane Policing (CoPP) on Aruba switches is used to mitigate Denial of Service (DoS) attacks on the switch. CoPP allows network administrators to restrict the impact of control plane traffic on the switch's CPU, thereby protecting network stability and integrity. By setting rate limits and specifying allowed traffic types, administrators can prevent malicious or malformed packets from overwhelming the switch's control plane, which could otherwise lead to a DoS condition and potentially disrupt network operations. This use case of CoPP is detailed in Aruba's network management documentation, where best practices and configurations to protect against DoS attacks are discussed.

Question 8

Question Type: MultipleChoice

What is a Key feature of me ArubaOS firewall?

Options:

A- The firewall is stateful which means that n can track client sessions and automatically allow return traffic for permitted sessions
B- The firewall Includes application layer gateways (ALGs). which it uses to filter Web traffic based on the reputation of the destination web site.
C- The firewall examines all traffic at Layer 2 through Layer 4 and uses source IP addresses as the primary way to determine how to control traffic.
D- The firewall is designed to fitter traffic primarily based on wireless 802.11 headers, making it ideal for mobility environments

Answer:

A

Explanation:

The ArubaOS firewall is a stateful firewall, meaning that it can track the state of active sessions and can make decisions based on the context of the traffic. This stateful inspection capability allows it to automatically allow return traffic for sessions that it has permitted, thereby enabling seamless two-way communication for authorized users while maintaining the security posture of the network. :

ArubaOS firewall documentation.