HP ACNSP HPE7-A02 Practice Questions

Shared by Drake on 17-08-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

How can HPE Aruba Networking User-Based Tunneling (UBT) help companies implement a Zero Trust Security strategy?

Options:

A- By extending internal security zones through integration with cloud-based security solutions
B- By controlling wired and wireless clients with consistent identity- and context-based access policies
C- By applying best-practice data center security technologies, such as VXLAN, all the way to the internal edge
D- By applying strong encryption to all traffic that flows through the corporate LAN

Answer:

B

Explanation:

User-Based Tunneling supports Zero Trust by allowing organizations to enforce consistent role-based policies for wired and wireless users. Instead of trusting a device because it is physically connected to the LAN, the network uses identity, role, and context to determine access. UBT can tunnel selected wired traffic from AOS-CX switches to gateways where centralized firewall policies are applied. This allows wired users to receive enforcement similar to wireless users. Zero Trust requires least-privilege access and consistent policy based on identity and device context, not broad network placement. UBT is not mainly about VXLAN, universal LAN encryption, or cloud-zone extension. Its main Zero Trust value is consistent identity-based access enforcement.

==========

Question 2

Question Type: MultipleChoice

A company uses both HPE Aruba Networking ClearPass Policy Manager (CPPM) and HPE Aruba Networking ClearPass Device Insight (CPDI).

What is one way integrating the two solutions can help the company implement Zero Trust

Security?

Options:

A- CPPM can provide CPDI with custom device fingerprint definitions in order to enhance the company's total visibility.
B- CPDI can provide CPPM with extra information about users' identity; CPPM can then use that information to apply the correct identity-based enforcement.
C- CPPM can inform CPDI that it has assigned a particular Aruba-User-Role to a client; CPDI can then use that information to reclassify the client.
D- CPDI can use tags to inform CPPM that clients are using prohibited applications; CPPM can then tell the network infrastructure to quarantine those clients.

Answer:

D

Explanation:

Integrating HPE Aruba Networking ClearPass Policy Manager (CPPM) and HPE Aruba Networking ClearPass Device Insight (CPDI) can help a company implement Zero Trust Security by allowing CPDI to use tags to inform CPPM that clients are using prohibited applications. CPPM can then take action, such as telling the network infrastructure to quarantine those clients, ensuring that only compliant and trusted devices have network access.

1.Device Insight Tags: CPDI can monitor client behavior and tag devices that are using prohibited applications.

2.Policy Enforcement: CPPM can use these tags to apply specific enforcement actions, such as quarantining non-compliant devices.

3.Zero Trust Implementation: This integration supports Zero Trust Security by ensuring that all devices are continuously monitored and controlled based on their behavior and compliance with security policies.

Question 3

Question Type: MultipleChoice

HPE Aruba Networking Central displays an alert about an Infrastructure Attack that was detected. You go to the Security > RAPIDS events and see that the attack

was "Detect adhoc using Valid SSID."

What is one possible next step?

Options:

A- Use HPE Aruba Networking Central floorplans or the detecting AP identities to locate the general area for the threat.
B- Look for the IP address associated with the offender and then check for that IP address among HPE Aruba Networking Central clients.
C- Make sure that you have tuned the threshold for that check, as false positives are common for it.
D- Make sure that clients have updated drivers, as faulty drivers are a common explanation for this attack type.

Answer:

A

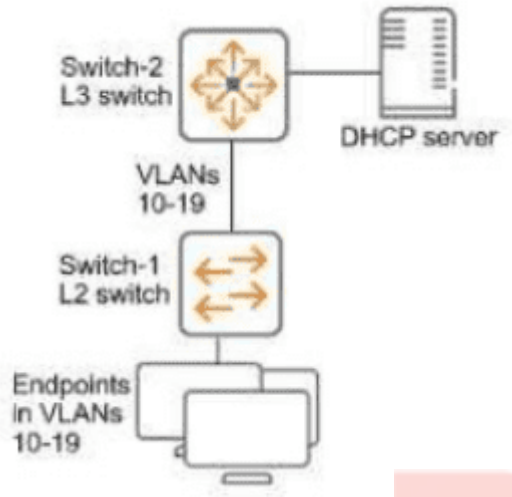
Explanation:

When HPE Aruba Networking Central detects an Infrastructure Attack, such as 'Detect adhoc using Valid SSID,' the next step is to locate the general area of the threat. You can use HPE Aruba Networking Central floorplans or the identities of the detecting APs to pinpoint the approximate location of the adhoc network. This allows you to physically investigate and address the source of the threat, ensuring that unauthorized or rogue networks are quickly identified and mitigated.

Question 4

Question Type: MultipleChoice

Refer to the exhibit.



You have verified that AOS-CX Switch-1 has constructed an IP-to-MAC binding table in VLANs 10-19. Now you need to enable ARP inspection for the endpoint connected to Switch-1. What must you do first to prevent traffic disruption?

Options:

A- Configure ARP inspection on VLANs 10-19 on Switch-2.
B- Configure DHCP snooping on VLANs 10-19 on Switch-2.
C- Configure Switch-1 uplinks as trusted ARP inspection ports.
D- Create a static IP-to-MAC binding on Switch-1 for the DHCP server.

Answer:

C

Explanation:

Dynamic ARP Inspection (DAI):

ARP inspection verifies ARP packets against a trusted IP-to-MAC binding table to prevent ARP spoofing attacks.

DHCP snooping is required to construct the IP-to-MAC binding table dynamically.

To avoid traffic disruption, uplink ports that connect to trusted switches, DHCP servers, or routers must be explicitly configured as trusted ports for ARP inspection.

Steps to Prevent Traffic Disruption:

Trust the Uplinks: ARP inspection must treat uplink ports as trusted to allow ARP traffic from legitimate DHCP servers and upstream switches.

Enable DHCP Snooping: DHCP snooping must be enabled on Switch-2 to ensure consistent IP-to-MAC bindings upstream.

Why the Answer is Correct:

Option A: Incorrect. ARP inspection on Switch-2 is important but not required first to prevent disruption on Switch-1.

Option B: Incorrect. DHCP snooping must be enabled upstream eventually, but this alone will not stop immediate traffic disruption on Switch-1.

Option C: Correct. Switch-1 uplinks must be trusted ARP inspection ports first to allow legitimate upstream traffic and prevent ARP disruption.

Option D: Incorrect. Static bindings are not required if DHCP snooping is enabled, and they are manual, limiting scalability.

Conclusion:

To avoid traffic disruption, configure Switch-1 uplinks as trusted ARP inspection ports to ensure valid ARP traffic can pass upstream and downstream.

Question 5

Question Type: MultipleChoice

A company has wired VolP phones, which transmit tagged traffic and connect to AOS-CX switches. The company wants to tunnel the phones' traffic to an HPE

Aruba Networking gateway for applying security policies.

What is part of the correct configuration on the AOS-CX switches?

Options:

A- UBT mode set to VLAN extend
B- A VXLAN VNI mapped to the VLAN assigned to the VolP phones
C- VLANs assigned to the VolP phones configured on the switch uplinks
D- A UBT reserved VLAN set to a VLAN dedicated for that purpose

Answer:

D

Explanation:

To tunnel VoIP phone traffic from AOS-CX switches to an HPE Aruba Networking gateway, you

need to configure a User-Based Tunneling (UBT) reserved VLAN on the switches. This VLAN is dedicated for tunneling purposes and ensures that the VoIP traffic is correctly identified and tunneled to the gateway where security policies can be applied.

1.UBT Configuration: Setting a UBT reserved VLAN ensures that the switch knows which VLAN to use for tunneling traffic to the gateway.

2.Traffic Tunneling: The reserved VLAN helps in segregating the VoIP traffic, ensuring it is handled securely and according to the configured policies at the gateway.

3.Policy Application: By tunneling the traffic, the gateway can apply advanced security policies to the VoIP traffic.

Question 6

Question Type: MultipleChoice

You need to use "Tips:Posture" conditions within an 802.1X service's enforcement policy.

Which guideline should you follow?

Options:

A- Enable caching roles and posture attributes from previous sessions in the service's enforcement settings.
B- Create rules that assign postures in the service's role mapping policy.
C- Enable profiling in the service's general settings.
D- Select the Posture Policy type for the service's enforcement policy.

Answer:

A

Explanation:

When using 'Tips

' conditions within an 802.1X service's enforcement policy, you should enable caching roles and posture attributes from previous sessions in the service's enforcement settings. This ensures that ClearPass retains posture information from previous authentications, which is necessary for making decisions based on the current posture state of an endpoint. By caching these attributes, ClearPass can apply appropriate enforcement actions based on the device's posture status.

Question 7

Question Type: MultipleChoice

A company has an HPE Aruba Networking ClearPass cluster with several servers. ClearPass Policy Manager (CPPM) is set up to:

. Update client attributes based on Syslog messages from third-party appliances

. Have the clients reauthenticate and apply new profiles to the clients based on the updates

To ensure that the correct profiles apply, What is one step you should take?

Options:

A- Configure a CoA action for all tag updates in the ClearPass Device Insight integration settings.
B- Tune the CoA delay on the ClearPass servers to a value of 5 seconds or greater.
C- Set the cluster's Endpoint Context Servers polling interval to a value of 5 seconds or less.
D- Configure the cluster to periodically clean up (delete) unknown endpoints.

Answer:

B

Explanation:

To ensure that the correct profiles apply after client attributes are updated based on Syslog messages, you should tune the Change of Authorization (CoA) delay on the ClearPass servers to a value of 5 seconds or greater. This delay allows sufficient time for the attribute updates to be processed and for the reauthentication to occur correctly, ensuring that the updated profiles are accurately applied to the clients.

1.CoA Delay: Adjusting the CoA delay ensures that the system has enough time to update client attributes and reauthenticate them properly before applying new profiles.

2.Profile Accuracy: This delay helps in preventing premature reauthentication and ensures that the most recent attribute updates are considered when applying profiles.

3.System Synchronization: Ensures synchronization between the attribute update and the reauthentication process.

Question 8

Question Type: MultipleChoice

You have created this rule in an HPE Aruba Networking ClearPass Policy Manager (CPPM) service's enforcement policy:

IF Authorization [Endpoints Repository] Conflict EQUALS true

THEN apply "quarantine_profile"

What information can help you determine whether you need to configure cluster-wide profiler parameters to ignore some conflicts?

Options:

A- Whether some devices are running legacy operating systems
B- Whether the company has rare Internet of Things (IoT) devices
C- Whether some devices are incapable of captive portal or 802.1X authentication
D- Whether the company has devices that use PXE boot

Answer:

D

Explanation:

A conflict in the Endpoints Repository usually indicates that ClearPass has seen different profiling data for the same MAC, which might mean a spoofing attempt---or simply normal behavior for certain device types.

Devices that use PXE boot often:

Boot initially from the network with one set of characteristics (e.g., a minimal OS, different DHCP fingerprint),

Then chain-load into a different OS with a different fingerprint and sometimes even a different network profile.

Aruba exam and design material specifically point out PXE boot as a common, benign cause of profiler conflicts and recommend tuning cluster-wide profiler parameters to ignore or relax some conflicts for these devices.

Therefore, you look at whether the company has devices that use PXE boot when deciding whether to tune profiler conflict behavior Option D.

Question 9

Question Type: MultipleChoice

A company has AOS-CX switches and HPE Aruba Networking APs, which run AOS-10 and bridge their SSIDs. Company security policies require 802.1X on all edge ports, some of which connect to APs. How should you configure the auth-mode on AOS-CX switches?

Options:

A- Leave all edge ports in client auth-mode and configure device auth-mode in the AP role.
B- Configure all edge ports in client auth-mode.
C- Configure all edge ports in device auth-mode.
D- Leave all edge ports in device auth-mode and configure client auth-mode in the AP role.

Answer:

A

Explanation:

802.1X Authentication Modes:

Client Auth-Mode: Requires each connected endpoint to authenticate individually using 802.1X.

Device Auth-Mode: Allows the port to authenticate a device, such as an AP, as a whole. This mode works when the device bridges traffic (e.g., AP bridging SSID traffic).

AP Role Configuration:

Since the AP bridges traffic from multiple clients, you must configure the AP role to use device auth-mode.

Meanwhile, the ports on edge switches can remain in client auth-mode to enforce 802.1X for individual client connections.

Option Analysis:

Option A: Correct. This ensures the AP itself authenticates with device auth-mode, while edge ports remain in client auth-mode.

Option B: Incorrect. APs require device auth-mode for bridging, not client auth-mode.

Option C: Incorrect. Device auth-mode on all ports would not meet the security policy for clients.

Option D: Incorrect. Leaving all ports in device auth-mode does not meet the policy for 802.1X

on edge ports.

P2P exams