HPE7-A10 Dumps

Shared by Gaines on 20-11-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

You are assisting a company with designing role-based access control policies on HPE Aruba Networking AOS-10 gateways. The security policy dictates that traffic originating from authenticated corporate user roles must be inspected statefully, allowing client-initiated outbound flows to the data center while strictly dropping any unsolicited inbound connection attempts initiated from data center servers back toward the clients.

What design principle ensures this traffic flow behavior?

Options:

A- Session ACLs on AOS-10 gateways are stateful and inherently permit return traffic while blocking unsolicited reverse sessions.
B- Gateways must have explicit inverse session rules configured matching the reverse TCP flags (ACK=1, SYN=0).
C- Administrators must deploy an external firewall because gateway PEF roles only enforce stateless Layer 2 filtering.
D- The gateway must be switched from Default Gateway mode to Mobility Access mode to enable bidirectional state tracking.

Answer:

A

Explanation:

In HPE Aruba Networking AOS-10 architectures, the Policy Enforcement Firewall (PEF) is an application-aware, stateful Layer 4--7 firewall embedded directly within the datapath of gateways and access points.

When an Access Control Entry (ACE) is defined within a user role's session ACL (for example, permitting traffic with user host 10.20.1.50 svc-https permit), the PEF datapath dynamically constructs a bidirectional stateful session flow entry in its hardware session table upon observing the client's initial TCP SYN or UDP packet.

Because the firewall tracks protocol states (including TCP sequence/acknowledgment numbers and UDP pseudo-sessions), it automatically permits corresponding return traffic returning from the destination server back to the client. Crucially, this stateful tracking is unidirectional with respect to session establishment: external hosts, including data center servers, cannot initiate new, unsolicited connections toward the client because no matching stateful session exists in the reverse direction. Engineers do not need to configure inverse rules, inspect raw TCP ACK flags, or

deploy secondary firewalls, as PEF enforces this stateful isolation by default.

Question 2

Question Type: MultipleChoice

A customer has an AOS-10 architecture that includes HPE Aruba Networking APs. The customer recently enabled WIDS at the high level on the APs. Administrators see several "ad hoc using valid SSID" events.

What should you explain?

Options:

A- A hacker could be trying to launch a man-in-the-middle or DoS attack. You will start tracking down the source of the events immediately.
B- Domain GPOs have likely misconfigured clients. You will meet with the domain admins to work out the issue.
C- The WIDS solution is likely malfunctioning, causing APs to detect each other as threats. You will check the configuration immediately.
D- Faulty client drivers often cause this event. You will look out for other events, but the customer should not worry.

Answer:

A

Explanation:

The 802.11 standard defines two primary operational modes: Infrastructure mode (where clients associate exclusively with an Access Point) and Independent Basic Service Set (IBSS), commonly known as Ad-Hoc mode (where stations communicate directly peer-to-peer without an AP).

The WIDS signature ad hoc using valid SSID triggers when a device transmits 802.11 beacon frames configured in Ad-Hoc/IBSS mode while advertising the enterprise's authorized, valid SSID name. In enterprise security, this is a serious threat indicator:

An attacker may be operating a software-defined Wi-Fi adapter broadcasting the corporate SSID in ad-hoc mode to trick adjacent client devices into establishing peer-to-peer associations, allowing the attacker to bypass access-layer firewalls and compromise connected endpoints directly.

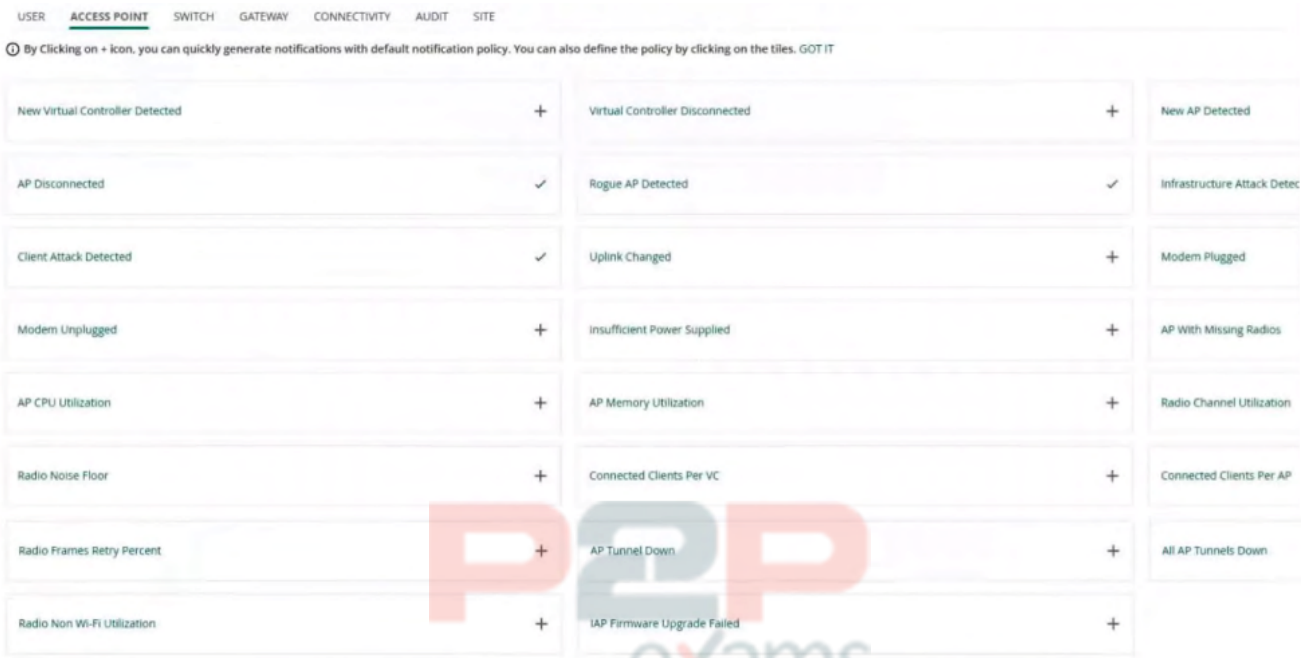
Alternatively, an attacker may be staging a Man-in-the-Middle (MitM) credential harvesting campaign or a Denial-of-Service (DoS) condition by poisoning the BSSID/channel mapping of legitimate corporate endpoints.

This event represents deliberate wireless framing manipulation rather than a routine client driver glitch or GPO misconfiguration. Security teams should treat this detection as an active threat, immediately triangulating the transmitting MAC address and RF location using Central/RAPIDS to locate and contain the source.

Question 3

Question Type: MultipleChoice

A customer uses an AOS-10 architecture that includes HPE Aruba Networking APs. Administrators recently enabled WIDS at the High level and also enabled alerts and email notifications for several events.



Administrators report receiving so many emails that they must ignore them and are considering disabling all notifications. What is one step you could recommend trying first?

Options:

A- Disable email notifications for Rogue AP, but leave the Infrastructure Attack Detected and Client Attack Detected notifications on.

B- Change the WIDS level to custom, and enable only the checks most likely to indicate real threats.

C- Send the email notifications directly to a specific folder, and only check the folder once a week.
D- Disable just the Rogue AP and Client Attack Detected alerts, as they overlap with the Infrastructure Attack Detected alert.

Answer:

B

Explanation:

In HPE Aruba Networking Central, configuring Wireless Intrusion Detection System (WIDS) at the High profile enables every available client and infrastructure detection signature. In real-world enterprise environments, aggressive signature sets (such as frame flood detectors, sequence number jumps, and client disconnect thresholds) generate frequent false positives caused by client driver bugs, background roaming, and RF noise. When paired with automated email alerting, this causes alert fatigue, often leading administrators to ignore alerts entirely.

Disabling critical alert classes (such as Rogue AP or Client Attack notifications) removes core defense-in-depth controls. The architecturally sound remediation is to transition the WIDS policy from the pre-packaged 'High' profile to the Custom profile.

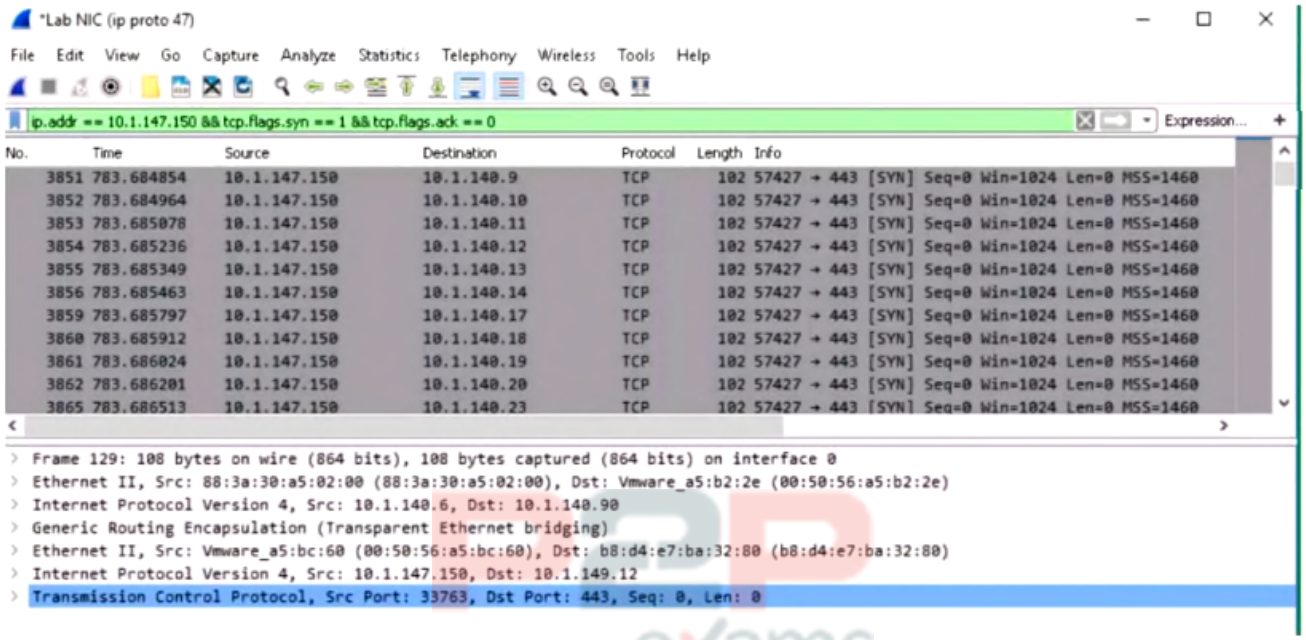
Under the Custom policy, security teams maintain granular control over individual detection engines. Administrators can disable high-noise, low-fidelity checks (such as EAP handshake timeouts or rate anomaly detection) while keeping high-confidence, actionable threat signatures enabled (such as AP spoofing, rogue AP detection, and evil twin attacks). This eliminates false alarms while preserving visibility into actionable threats.

Question 4

Question Type: MultipleChoice

Refer to the exhibit.

An administrator has configured a remote mirror between an AOS-CX switch and a station running a protocol analyzer. The exhibit displays a sample of the packet capture.



Packet trace details:

Source: 10.1.147.150 -> Destination: 10.1.140.9 TCP 57427 -> 443 [SYN] Seq=0 Len=0

Source: 10.1.147.150 -> Destination: 10.1.140.10 TCP 57427 -> 443 [SYN] Seq=0 Len=0

Source: 10.1.147.150 -> Destination: 10.1.140.11 TCP 57427 -> 443 [SYN] Seq=0 Len=0

Source: 10.1.147.150 -> Destination: 10.1.140.12 TCP 57427 -> 443 [SYN] Seq=0 Len=0

Source: 10.1.147.150 -> Destination: 10.1.140.13 TCP 57427 -> 443 [SYN] Seq=0 Len=0

Packet encapsulation tree shows Generic Routing Encapsulation (Transparent Ethernet bridging).

Which characteristic is suspicious?

Options:

A- The fact that 10.1.147.150 is trying to connect to many different devices
B- The TCP flags in these packets, which do not occur in innocent packets
C- The excessively small size of many of these packets
D- The fact that traffic is encapsulated by GRE, a sign of command and control tunnels

Answer:

A

Explanation:

The Wireshark capture illustrates a clear pattern of horizontal network scanning / host discovery.

Endpoint 10.1.147.150 is systematically generating initial TCP connection requests (SYN frames) targeting a single destination service (HTTPS port 443) across sequential destination IP addresses in rapid succession (10.1.140.9, .10, .11, .12, .13, .14, etc.).

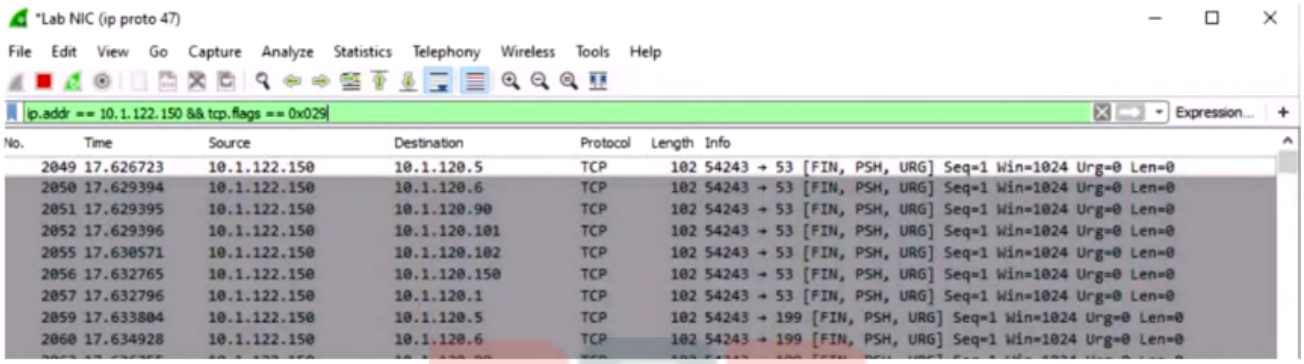
In legitimate client behavior, endpoints do not systematically iterate through consecutive IP addresses on a subnet attempting to establish SSL/TLS handshakes across identical source and destination ports within milliseconds. This behavior is indicative of automated network reconnaissance or an infected host attempting lateral movement and worm propagation.

The other technical characteristics observed in the trace are normal: TCP SYN packets routinely have a length of 0 with no payload; TCP flags (SYN=1, ACK=0) are standard for initial session handshakes; and Generic Routing Encapsulation (GRE) is expected because the administrator configured remote port mirroring (ERSPAN) on the AOS-CX switch to deliver mirrored packets to the analyzer station.

Question 5

Question Type: MultipleChoice

Refer to the exhibit.



Packet trace display:

Source: 10.1.122.150 -> Destination: 10.1.120.5 TCP 54243 -> 53 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0

Source: 10.1.122.150 -> Destination: 10.1.120.6 TCP 54243 -> 53 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0

Source: 10.1.122.150 -> Destination: 10.1.120.90 TCP 54243 -> 53 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0

Source: 10.1.122.150 -> Destination: 10.1.120.101 TCP 54243 -> 53 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0

Source: 10.1.122.150 -> Destination: 10.1.120.5 TCP 54243 -> 199 [FIN, PSH, URG] Seq=1

Win=1024 Urg=0 Len=0

What does this indicate?

Options:

A- Someone is attempting to determine which ports are open on devices in subnet 10.1.120.0/24.
B- Someone is attempting to launch a DoS attack against clients in the 10.1.120.0/24 subnet.
C- Port forwarding policies are misconfigured on core routers or routing switches.
D- A hacker is hijacking the connections between clients in 10.1.120.0/24 and the true owner of the 10.1.122.150 IP address.

Answer:

A

Explanation:

The Wireshark display filter tcp.flags == 0x029 isolates TCP packets where the FIN (bit 0x001), PSH (bit 0x008), and URG (bit 0x020) control bits are simultaneously set (0x001 + 0x008 + 0x020 = 0x029). In network security and reconnaissance analysis, this combination of flags is the definition of a TCP Xmas Tree Scan.

Under RFC 793 specifications, any closed TCP port receiving a packet that lacks a SYN, ACK, or RST bit must respond with a TCP RST frame, whereas an open listening port is required to silently drop the packet. Scanning tools (such as Nmap) utilize Xmas scans to probe target operating systems and determine port states while attempting to bypass stateless access control lists and legacy firewalls.

The exhibit demonstrates host 10.1.122.150 sequentially transmitting Xmas probes to multiple consecutive host IP addresses (10.1.120.5, 10.1.120.6, 10.1.120.90, etc.) across various destination ports (such as port 53 and port 199). This confirms active network reconnaissance attempting to identify open services on subnet 10.1.120.0/24.

Question 6

Question Type: MultipleChoice

The customer needs a secure wireless solution that lets users onboard new wireless clients. You are recommending a new WLAN that will give users limited access for this process.

Which WLAN security should you recommend, assuming users have a mixture of WPA2- and

WPA3-capable devices?

Options:

A- Open with MAC Authentication
B- WPA3-Personal with backward compatibility to WPA2
C- Enhanced Open without backward compatibility
D- WPA3-Enterprise with 128-bit keys

Answer:

B

Explanation:

When provisioning an onboarding or provisioning SSID designed to accommodate un-enrolled personal endpoints, the wireless infrastructure must provide baseline over-the-air cryptographic protection while ensuring broad compatibility across heterogeneous client hardware.

Configuring WPA3-Personal with backward compatibility to WPA2 (commonly designated as WPA3-Personal Transition Mode) satisfies both operational criteria:

Modern devices supporting WPA3 negotiate Simultaneous Authentication of Equals (SAE), securing the association against offline dictionary attacks and providing forward secrecy.

Legacy endpoints that only support WPA2-Personal associate using standard WPA2-PSK (Pre-Shared Key) handshakes on the same SSID.

This transitional capability allows enterprise users to connect their diverse personal devices to the onboarding network to complete enrollment and certificate provisioning. In contrast, Enhanced Open without backward compatibility breaks connectivity for legacy clients that do not support Opportunistic Wireless Encryption (OWE), while pure Open networks provide no RF encryption. WPA3-Enterprise requires operational 802.1X supplicant configurations and certificates upfront, which clients do not yet possess prior to onboarding.

Question 7

Question Type: MultipleChoice

You are entering the following command on an AOS-CX switch:

radius-server host clearpass.example.com tls clearpass-username clearpass-password plaintext

Which credentials should you enter for clearpass-username and clearpass-password?

Options:

A- the credentials for a CPPM admin with HPE Aruba Networking Role Download privileges
B- the RADIUS secret configured in the corresponding network device entry on CPPM
C- the username in the certificate that the switch uses for Radsec and the password for the certificate's private key
D- the credentials of a user account used for RADIUS server tracking

Answer:

A

Explanation:

In AOS-CX switches utilizing Dynamic Segmentation and Downloadable User Roles (DUR), client authentication occurs via standard RADIUS, but the actual retrieval of the role definition, classes, and policy ACLs is performed out-of-band via secure RESTful HTTPS API calls back to ClearPass Policy Manager.

When configuring the switch to communicate with ClearPass for downloadable user roles, the radius-server host <FQDN> tls <username> plaintext command provisions the administrative credentials that the switch uses to authenticate to ClearPass's REST API endpoint during role download operations.

ClearPass Policy Manager implements granular role-based administrative privilege controls. Best practice mandates creating an administrative service account in CPPM assigned the restricted administrative privilege profile: HPE Aruba Networking Role Download. These credentials permit the switch to authenticate over HTTPS and download the compiled role configuration without granting broader administrative rights to modify ClearPass policies, server configurations, or user repositories. These credentials are distinct from the RADIUS shared secret or RadSec TLS certificates.

Question 8

Question Type: MultipleChoice

You are configuring gateway IDS/IPS settings in HPE Aruba Networking Central.

Why would you set the Fail Strategy to Bypass?

Options:

A- To tell gateways to stop enforcing IDS/IPS policies if they lose connectivity to the Internet
B- To enable the gateway to honor the allowlist settings configured in IDS/IPS policies
C- To permit traffic if the IPS engine fails to inspect it
D- To avoid wasting IPS engine resources on filtering traffic for unauthenticated clients

Answer:

C

Explanation:

On HPE Aruba Networking Branch and Campus Gateways, the Gateway IDS/IPS subsystem executes inline deep packet inspection (DPI) and signature matching using a dedicated software container engine. The Fail Strategy configuration parameter governs the forwarding plane behavior in the catastrophic event that the IPS inspection engine experiences a failure, software crash, internal timeout, or severe memory/processing exhaustion.

ArubaOS provides two operational fail strategies:

Block (Fail-Closed): If the IPS engine fails or becomes unresponsive, all traffic requiring inspection is dropped. This ensures maximum security but risks severe service disruption during engine faults.

Bypass (Fail-Open): If the IPS engine fails or is unable to process incoming packets, the gateway bypasses the inspection pipeline, forwarding packets directly through standard routing and firewall switching paths without deep threat inspection.

Setting the Fail Strategy to Bypass prioritizes business continuity and network availability over strict security enforcement, preventing network downtime in the event of an IPS engine fault.

To Get Premium Files for HPE7-A10 Visit
https://www.p2pexams.com/products/hpe7-a10

For More Free Questions Visit
https://www.p2pexams.com/hp/pdf/hpe7-a10

