DUMPSBOSS.

Aruba Certified Network Security Professional Exam

HP HPE7-A02

Version Demo

Total Demo Questions: 16

Total Premium Questions: 168

Buy Premium PDF

https://dumpsboss.co

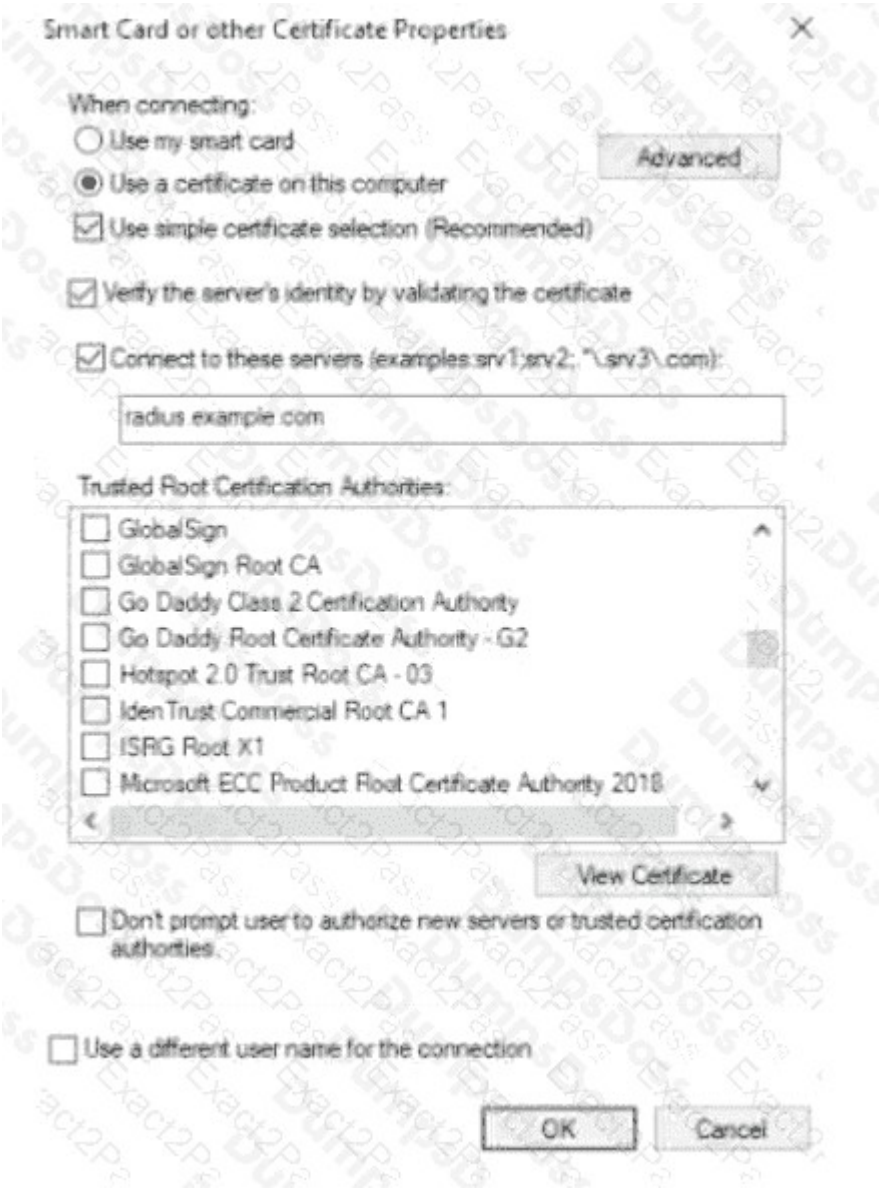
support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

Topic Break Down

Topic	No. of Questions
Topic 1, Network Security Fundamentals	6
Topic 2, Aruba Security Products and Solutions	46
Topic 3, Security Design	1
Topic 4, Security Implementation	95
Topic 5, Security Troubleshooting	20
Total	168

QUESTION NO: 1



The exhibit shows the 802.1X-related settings for Windows domain clients. What should admins change to make the settings follow best security practices?

A. Specify at least two server names under the " Connect to these servers " field.

B. Select the desired Trusted Root Certificate Authority and select the check box next to " Don ' t prompt users. "

C. Under the " Connect to these servers " field, use a wildcard in the server name.

D. Clear the check box for using simple certificate selection and select the desired certificate manually.

ANSWER: B

Explanation:

Select the desired Trusted Root Certificate Authority and select the check box next to " Don ' t prompt users. " This enforces validation of the authentication server certificate during protected EAP authentication. A Windows supplicant must trust the certification authority that issued the RADIUS server certificate before it can establish the protected tunnel used for credential authentication. Restricting trust to the appropriate root certification authority prevents a client from treating an arbitrary certificate chain as acceptable.

Enabling the setting that prevents user prompts is equally important because users should not be asked to decide whether an unexpected server certificate is safe. If a certificate-validation warning is exposed to an end user, the user may accept an

untrusted certificate, which can enable credential-harvesting attacks through a rogue wireless access point or authentication server. The configuration should therefore use centrally managed trust settings and require successful server-certificate validation without user override. Microsoft describes the role of certificate validation in protected EAP deployment in its Network Policy Server EAP configuration documentation. Aruba also recommends validating the authentication server certificate and trusted issuer as part of secure enterprise wireless deployment in the ClearPass 802.1X authentication documentation.

QUESTION NO: 2

A company wants to turn on Wireless IDS/IPS infrastructure and client detection at the high level on HPE Aruba Networking APs. The company does not want to

enable any prevention settings.

What should you explain about HPE Aruba Networking recommendations?

A. HPE Aruba Networking recommends turning on both wired and wireless prevention whenever you enable detection at high.

B. HPE Aruba Networking recommends using hybrid AP mode, as opposed to Air Monitors (AMs), when implementing detection without prevention.

C. HPE Aruba Networking recommends disabling client detection when you configure infrastructure detection at high, as infrastructure detection includes all the client checks and more.

D. HPE Aruba Networking recommends configuring infrastructure and client detection at a custom level and disabling or tuning some of the settings that are likely to produce false positives.

ANSWER: D

Explanation:

HPE Aruba Networking recommends configuring infrastructure and client detection at a custom level and disabling or tuning some of the settings that are likely to produce false positives. The High detection level enables a broad set of wireless IDS checks, which provides extensive visibility but can generate alerts for behavior that is legitimate in a particular RF environment. This is especially relevant when the organization wants detection and reporting only, rather than automatically taking containment or other prevention actions.

A custom profile lets administrators retain the infrastructure and client checks that are useful for their risk profile while tuning checks whose thresholds, signatures, or alert conditions are too sensitive for the local deployment. This produces more actionable alerts, reduces operational noise, and helps security staff investigate genuine wireless threats without alert fatigue. Aruba documentation describes Wireless IDS capabilities for detecting both infrastructure and client-related events, and supports configuring detection settings to meet the needs of the deployment. See the ArubaOS Wireless IDS/WIPS documentation and the Aruba Central WIDS documentation.

QUESTION NO: 3

You have created this rule in an HPE Aruba Networking ClearPass Policy Manager (CPPM) serviceâ€™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?

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:

Whether the company has devices that use PXE boot is the information that helps determine whether selected profiler conflicts should be ignored at the cluster level. ClearPass Profiler builds endpoint classifications from observations such as DHCP characteristics, network behavior, and other discovered attributes. A repository conflict is raised when the same endpoint MAC address is associated with differing profiling information. This can be valuable for detecting unexpected identity changes, but not every difference represents a security event.

PXE boot is a common legitimate reason for a device to present substantially different attributes over a short period. During its initial network boot, a workstation can use a preboot execution environment with a DHCP fingerprint and behavior distinct from those of the operating system it loads afterward. Once the full operating system starts, ClearPass can observe a new fingerprint or profile for the same MAC address and record a conflict. If this behavior is expected in the environment, administrators can use the cluster-wide profiler conflict settings to ignore the relevant benign differences, preventing normal PXE workflows from triggering the quarantine enforcement profile. Aruba's ClearPass documentation describes endpoint profiling and repository-based endpoint attributes in the ClearPass Policy Manager documentation; additional ClearPass technical resources are available through the HPE Aruba Networking TechDocs portal.

QUESTION NO: 4

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?

A. Make sure that you have tuned the threshold for that check as false positives are common for it.

B. Make sure that clients have updated drivers, as faulty drivers are a common explanation for this attack type.

C. Use HPE Aruba Networking Central floorplans or the detecting AP identities to locate the general area for the threat.

D. Look for the IP address associated with the offender and then check for that IP address among HPE Aruba Networking Central clients.

ANSWER: C

Explanation:

Use HPE Aruba Networking Central floorplans or the detecting AP identities to locate the general area for the threat. The "Detect adhoc using Valid SSID" event identifies an ad hoc wireless network advertising an SSID that matches one configured or recognized as valid in the environment. Because this can indicate an unauthorized device attempting to imitate a trusted wireless network name, the immediate operational priority is to establish where the radio signal is being observed and investigate the physical device responsible.

Central RAPIDS events provide the APs that detected the wireless device, and those AP identities can be correlated with AP placement, floorplans, and signal observations. If a floorplan is available and AP locations are accurately maintained, it gives the security or wireless operations team a practical starting area for a site walk and device identification. This response supports physical verification and appropriate incident handling while retaining the RAPIDS event details as evidence.

Aruba describes RAPIDS as the Central capability for monitoring wireless threats and classifying potentially unauthorized devices. See Aruba Central RAPIDS documentation and Aruba Central RAPIDS events documentation.

QUESTION NO: 5

Which use case is fulfilled by applying a time range to a firewall rule on an AOS device?

A. Enforcing the rule only during the specified time range

B. Tuning the session timeout for sessions established with this rule

C. Locking clients that violate the rule for the specified time range

D. Setting the time range over which hit counts for the rule are aggregated

ANSWER: A

Explanation:

Enforcing the rule only during the specified time range is correct because a time range acts as a schedule associated with a firewall policy rule. The configured schedule defines when the rule is in effect, such as particular days of the week and start/end times. While the time range is active, traffic matching the rule is processed according to that rule's configured action and policy conditions. When the configured period is not active, the rule is not applied on the basis of that schedule.

This lets an administrator make firewall enforcement match an organization's operational timetable without manually enabling and disabling rules. For example, a policy can be scheduled to control access to an internal service during business hours, or a more restrictive access policy can be activated during a maintenance window. The feature is therefore a policy-scheduling mechanism: its purpose is to control *when* the firewall rule is enforced.

ArubaOS firewall documentation describes time ranges as reusable schedule objects that can be applied to firewall policies. See the ArubaOS Firewall Configuration documentation and the Configuring Time Ranges documentation.

QUESTION NO: 6

A company is using HPE Aruba Networking ClearPass Policy Manager (CPPM) and HPE Aruba Networking ClearPass Device Insight (CPDI). CPDI and CPPM are integrated. The security staff wants you to show them a list of all devices that are contacting a specific known command-and-control center.

What should you do?

A. In CPPM's Access Tracker, filter for that destination.

B. Use ClearPass Insight to run an Active Endpoint Security report.

C. In CPDI, look in Generic Device clusters based on that destination.

D. In CPDI, filter for that destination and save the filter as a tag.

ANSWER: D

Explanation:

In CPDI, filter for that destination and save the filter as a tag. is correct because ClearPass Device Insight continuously analyzes endpoint network behavior, including the destinations with which devices communicate. This makes it appropriate for an investigation centered on a known command-and-control destination: an administrator can use the destination as a filter to identify the devices exhibiting that communication pattern. The resulting filtered device population provides the requested list of affected endpoints rather than merely an individual authentication event or a static inventory grouping.

Saving the filtered results as a tag creates a reusable, meaningful classification for the identified devices. Tags support continued investigation and operational response by preserving the set of endpoints associated with the suspicious destination. In an integrated ClearPass deployment, device context and classification can also be used to inform downstream access-control or remediation workflows. This approach aligns device-behavior visibility with policy enforcement, allowing the security team to investigate the command-and-control indicator and retain a clear endpoint grouping for subsequent action. Aruba describes Device Insight as providing device discovery, profiling, and behavioral insights, while ClearPass provides policy-based access control and response capabilities. See the HPE Aruba Networking ClearPass overview and Aruba Central Device Insight documentation.

QUESTION NO: 7

HPE Aruba Networking ClearPass Device Insight (CPDI) could not classify some endpoints using system and user rules. Using machine learning, it did assign those endpoints to a cluster and discover a recommendation. In which of these circumstances does CPDI automatically classify the endpoints based on that recommendation?

A. The recommendation has 96% confidence, and it is based on 13 classified devices.

B. The recommendation has 98% confidence, and it is based on 5 classified devices.

C. The recommendation has 93% confidence, and it is based on 36 classified devices.

D. The recommendation has 100% confidence, and it is based on 4 classified devices.

ANSWER: A

Explanation:

The recommendation has 96% confidence, and it is based on 13 classified devices.

ClearPass Device Insight uses its machine-learning clustering process to identify endpoints with similar observed characteristics and to generate a likely classification recommendation. Automatic classification is deliberately restricted to recommendations that have sufficiently strong evidence, rather than simply assigning every cluster's suggested identity. The recommendation must meet the high-confidence threshold of at least 95%, and the cluster must have enough classified-device evidence to support that result—at least 10 classified devices. This combination provides both a strong calculated confidence value and a meaningful sample of already classified endpoints on which the recommendation is based.

Here, 96% exceeds the required confidence level and 13 classified devices exceeds the minimum evidence requirement. CPDI can therefore automatically apply the recommended classification to the previously unclassified endpoints in that cluster. This behavior helps maintain reliable endpoint profiling while allowing high-quality machine-learning results to reduce manual classification work. Aruba describes Device Insight's use of AI and machine learning for device discovery and classification in its ClearPass product information and provides product documentation through the Aruba TechDocs portal.

QUESTION NO: 8

A company has wired VoIP 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?

A. UBT mode set to VLAN extend

B. A VXLAN VNI mapped to the VLAN assigned to the VoIP phones

C. VLANs assigned to the VoIP phones configured on the switch uplinks

D. A UBT reserved VLAN set to a VLAN dedicated for that purpose

ANSWER: A

Explanation:

UBT mode set to VLAN extend is required for this use case. User-Based Tunneling on AOS-CX can operate in VLAN-extend mode to carry traffic from a specified client VLAN across a tunnel to an HPE Aruba Networking gateway. This is appropriate for wired VoIP phones that place their voice packets in a tagged voice VLAN: the switch identifies traffic in the configured VLAN and extends that VLAN to the gateway through the UBT tunnel.

At the gateway, the tunneled client traffic can be processed under the applicable gateway policies, including role-based firewall policy and other security controls. VLAN-extend mode is especially useful when policy enforcement is required centrally at the gateway while the endpoint remains connected to an access-switch port and uses a tagged VLAN. The switch configuration also includes the UBT zone and gateway/controller details, plus assignment of the relevant voice VLAN to the UBT configuration; setting the UBT mode to VLAN extend is the key mode selection that enables this VLAN-based tunneling behavior.

See the AOS-CX Security Guide and the Aruba Central User-Based Tunneling documentation for UBT and VLAN-extension configuration concepts.

QUESTION NO: 9

A company needs you to integrate HPE Aruba Networking ClearPass Policy Manager (CPPM) with HPE Aruba Networking ClearPass Device Insight (CPDI).

What is one task you should do to prepare?

A. Install the root CA for CPPM ' s HTTPS certificate as trusted in the CPDI application.

B. Configure WMI, SSH, and SNMP external accounts for device scanning on CPPM.

C. Enable Insight in the CPPM server configuration settings.

D. Collect a Data Collector token from HPE Aruba Networking Central.

ANSWER: A

Explanation:

Install the root CA for CPPM ' s HTTPS certificate as trusted in the CPDI application. The ClearPass Device Insight integration communicates with ClearPass Policy Manager over HTTPS, so Device Insight must be able to validate the TLS certificate that CPPM presents. Before configuring the connection, ensure that the certificate chain is trusted by importing the root certificate authority that issued the CPPM HTTPS server certificate into the trusted-certificate area of the Device Insight application. If an intermediate CA issued the CPPM certificate, the complete chain should also be available as required by the deployment. This preparation step establishes authenticated, encrypted communication between the services and prevents certificate-validation failures when CPDI connects to CPPM. It is particularly important when CPPM uses an enterprise PKI or another private CA, because that issuing authority is not necessarily in the standard public trust store. Aruba's Device Insight documentation covers the requirements and configuration workflow for integrating ClearPass Policy Manager, while ClearPass documentation describes certificate trust and HTTPS certificate management. See the HPE Aruba Networking Central Device Insight documentation and the ClearPass certificate trust-list documentation.

QUESTION NO: 10

You are setting up HPE Aruba Networking SSE. Which use case requires you to apply a non-default device posture in a rule?

A. Applying threat inspection to users when they access certain websites

B. Checking whether a client has antivirus software as a condition for receiving access to resources

C. Redirecting compromised clients to a remediation server

D. Integrating with HPE Aruba Networking ClearPass OnGuard

ANSWER: B

Explanation:

Checking whether a client has antivirus software as a condition for receiving access to resources is the use case that requires a non-default device posture. Device-posture policy lets HPE Aruba Networking SSE evaluate endpoint-security attributes before it grants access to protected applications or resources. A default posture does not express a specific, organization-defined endpoint requirement such as the presence and status of an antivirus product. To make antivirus a condition of access, an administrator must use a posture definition that evaluates the relevant endpoint attribute and apply that posture in the access rule.

This enables policy decisions based on the device's current security state, rather than solely on user identity, destination, or network context. When the endpoint meets the configured antivirus requirement, the rule can allow the intended access; the posture result is therefore an essential input to the access decision. This approach supports zero-trust access principles by

validating both the authenticated user and the security characteristics of the device used by that user. Aruba SSE documentation and solution resources are available through the HPE Aruba Networking SSE documentation portal and the Aruba SSE data sheet.

QUESTION NO: 11

A company uses HPE Aruba Networking ClearPass Policy Manager (CPPM) and HPE Aruba Networking ClearPass Device Insight (CPDI) and has integrated the

two. CPDI admins have created a tag. CPPM admins have created rules that use that tag in the wired 802.1X and wireless 802.1X services' enforcement policies.

The company requires CPPM to apply the tag-based rules to a client directly after it learns that the client has that tag.

What is one of the settings that you should verify on CPPM?

A. The "Device Sync" setting is set to 1 in the ClearPass Device Insight Integration settings.

B. Both 802.1X services have the "Profile Endpoints" option enabled and an appropriate CoA profile selected in the Profiler tab.

C. Both 802.1X services have the "Use cached Role and Posture attributes from the previous sessions" setting.

D. The "Polling Interval" is set to 1 in the ClearPass Device Insight Integration settings.

ANSWER: B

Explanation:

Both 802.1X services have the "Profile Endpoints" option enabled and an appropriate CoA profile selected in the Profiler tab. This is the required service-level configuration for ClearPass Policy Manager to react when endpoint information, including information synchronized from ClearPass Device Insight, changes after the original authentication. Enabling endpoint profiling causes ClearPass to maintain and evaluate the endpoint’s profiling data as part of the service workflow. The Device Insight tag can then be available for the enforcement-policy conditions configured by the administrator.

An appropriate Change of Authorization profile is equally important for the immediate requirement. After ClearPass learns the new tag and the endpoint’s applicable enforcement result changes, CoA allows ClearPass to instruct the access device—such as an Aruba switch or wireless controller—to reauthorize the already connected client. The client is therefore reevaluated against the wired or wireless 802.1X service without waiting for a normal reconnect, session timeout, or a later authentication event. This combines Device Insight tag synchronization with dynamic enforcement at the network-access layer. Aruba describes ClearPass Policy Manager as providing context-aware policy enforcement in its ClearPass product documentation; the ClearPass Policy Manager documentation provides the related service and profiler configuration guidance.

QUESTION NO: 12

A company has HPE Aruba Networking APs and AOS-CX switches, as well as HPE Aruba Networking ClearPass. The company wants CPPM to have HTTP User-

Agent strings to use in profiling devices.

What can you do to support these requirements?

A. Add the CPPM server's IP address to the IP helper list in all client VLANs on routing switches.

B. Schedule periodic subnet scans of all client subnets on CPPM.

C. Configure mirror sessions on the APs and switches to copy client HTTP traffic to CPPM.

D. On the APs and switches, configure a redirect to ClearPass Guest in the role for devices being profiled.

ANSWER: D

Explanation:

On the APs and switches, configure a redirect to ClearPass Guest in the role for devices being profiled. This enables ClearPass to obtain HTTP User-Agent information during the client's web interaction with the captive-portal service. An HTTP request includes headers sent by the endpoint, and the User-Agent header can provide useful profiling evidence, such as the endpoint's operating system family, browser, or embedded device client. ClearPass Policy Manager's profiling function combines such observed attributes with information from other sources to classify endpoints and apply policy based on the resulting endpoint category.

The redirect must be applied by the access infrastructure to the client role being profiled so that the client's HTTP request reaches the ClearPass Guest web service. ClearPass can then inspect the request metadata as part of the web-login/redirect workflow and use the User-Agent value as profiling input. This is an access-control and web-traffic redirection function, rather than a DHCP relay configuration: HTTP User-Agent data is carried in HTTP headers and is available when the endpoint accesses the redirected web service. Aruba's ClearPass documentation describes profiling as using endpoint attributes collected from multiple data sources, while the Guest documentation covers web-login and captive-portal workflows. See ClearPass Policy Manager profiling overview and ClearPass Guest overview.

QUESTION NO: 13

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?

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:

Whether the company has devices that use PXE boot is the relevant information. ClearPass Profiler correlates observations such as DHCP characteristics, network behavior, and other collected endpoint attributes to classify a device associated with a MAC address. A repository conflict can occur when subsequent observations for that same MAC appear to describe different device types or operating environments. Although this can be a useful indicator of an unexpected change or possible MAC-address spoofing, PXE is a common legitimate situation in which the endpoint's observed identity changes during startup.

A PXE-capable computer first boots into a minimal preboot environment to obtain an address and download its boot image. It can then start its installed operating system, which presents a different DHCP fingerprint and other profiling characteristics. Consequently, ClearPass can see conflicting profile evidence for one endpoint even though there is no security incident. Knowing whether PXE deployment or imaging workflows exist lets the administrator decide whether cluster-wide Profiler conflict-handling parameters should ignore the expected PXE-related conflicts, rather than unnecessarily applying the quarantine enforcement profile to managed systems during deployment or reimaging.

See Aruba's ClearPass Profiler overview and Profiler configuration documentation.

QUESTION NO: 14

You are setting up HPE Aruba Networking SSE to prohibit users from uploading and downloading files from Dropbox. What is part of the process?

A. Adding a web category that includes Dropbox

B. Installing the HPE Aruba Networking SSE root certificate on clients

C. Deploying a connector that can reach the remote users

D. Deploying a connector that can reach Dropbox

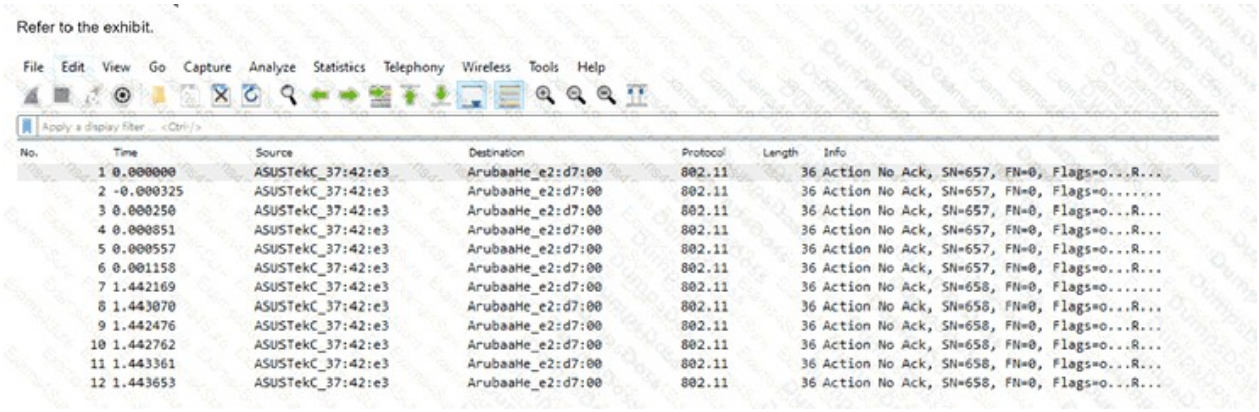
ANSWER: B

Explanation:

Installing the HPE Aruba Networking SSE root certificate on clients is part of the process because Dropbox transfers use HTTPS. To apply policy at the level needed to identify and control encrypted Dropbox activity, SSE must be able to perform TLS inspection. The client must trust the SSE root certificate so that SSE can decrypt the HTTPS session for inspection, enforce the configured application or web policy, and then re-encrypt the session without generating certificate-trust errors for the user. In a managed environment, administrators normally deploy this trusted root certificate through endpoint-management tooling, group policy, or the SSE client deployment workflow before enabling policies that require TLS decryption. This establishes the trusted inspection path that makes visibility into encrypted cloud-service traffic possible and allows the policy to prevent the intended Dropbox file-transfer behavior. Aruba describes SSE as providing security controls for internet and SaaS access, including inspection and policy enforcement for encrypted traffic; see the HPE Aruba Networking SSE overview and the Secure Service Edge For Dummies guide.

QUESTION NO: 15

Refer to the exhibit.



You have downloaded a packet capture that you generated on HPE Aruba Networking Central. When you open the capture in Wireshark, you see the output shown in the

exhibit.

What should you do in Wireshark so that you can better interpret the packets?

A. Choose to decode UDP port 5555 packets as ARUBA_ERM and set the Aruba ERM Type to 0.

B. Edit preferences for IEEE 802.11 and chose to ignore the Protection bit with IV.

C. Apply the following display filter: wlan.fc.type == 1.

D. Edit the Enabled Protocols and make sure that 802.11, GRE, and Aruba_ERM are enabled.

ANSWER: A

Explanation:

Choose to decode UDP port 5555 packets as ARUBA_ERM and set the Aruba ERM Type to 0. Aruba remote packet captures can use Aruba Encapsulated Remote Mirroring (ARUBA_ERM), which wraps the mirrored wireless traffic in a UDP-based encapsulation. If Wireshark does not associate the UDP stream with the ARUBA_ERM dissector, it displays only the outer UDP payload rather than decoding the encapsulated frames. Using Wireshark's *Decode As* capability for UDP port 5555 explicitly assigns the correct dissector to that traffic.

The Aruba ERM Type preference determines the kind of payload carried inside the ERM header. Setting the type to 0 directs Wireshark to interpret the encapsulated payload as the appropriate raw wireless packet format, enabling useful 802.11-level decoding and analysis of the capture. Once the ERM wrapper is decoded, Wireshark can expose the inner protocol fields and frame details needed to troubleshoot wireless behavior. Wireshark documents the ARUBA_ERM dissector and its preferences at ARUBA_ERM protocol reference. General instructions for mapping traffic to a dissector are available in the Wireshark User's Guide.

QUESTION NO: 16

What is a use case for running periodic subnet scans on devices from HPE Aruba Networking ClearPass Policy Manager (CPPM)?

A. Using DHCP fingerprints to determine a client ' s device category and OS

B. Detecting devices that fail to comply with rules defined in CPPM posture policies

C. Identifying issues with authenticating and authorizing clients

D. Using WMI to collect additional information about Windows domain clients

ANSWER: D

Explanation:

Using WMI to collect additional information about Windows domain clients is a valid use case for periodic subnet scans in ClearPass Policy Manager. ClearPass can use configured subnet scans to discover and profile endpoints that are present on a network segment. For Windows systems joined to a domain, a Windows Management Instrumentation (WMI) scan can query the endpoint using supplied domain credentials and collect endpoint attributes that are useful for profiling and policy decisions. This adds device context beyond the information available from a single network-access transaction.

Running the scan on a recurring schedule keeps ClearPass endpoint records current as devices are added, moved, or change state. The resulting attributes can improve endpoint classification and provide administrators with a more complete inventory of managed Windows clients. This is particularly useful where devices might not generate enough direct authentication or network telemetry for ClearPass to build a sufficiently detailed profile without an active scan. ClearPass documentation describes subnet scanning as a profiler capability and includes WMI-based collection for applicable Windows endpoints. See the ClearPass Policy Manager Endpoint Profiler documentation and the Endpoint Profiler overview.