ATMIC NETWORKS
YOUR GUIDE TO GLOBAL CERTIFIATION

"Please note that these files may not be up to date. However, the questions will help you understand the exam format and typical question patterns."

www.atmicnetworks .com

Warning: Keep connected with our support team for latest updates

Question: 1

You have configured an AOS-CX switch to implement 802.1X on edge ports. Assume ports operate in the default auth-mode. VoIP phones are assigned to the "voice" role and need to send traffic that is tagged for VLAN 12.

Where should you configure VLAN 12?

A. As the trunk native VLAN on edge ports and the trunk native VLAN on the "voice" role

B. As a trunk allowed VLAN on edge ports and the trunk native VLAN in the "voice" role

C. As the trunk native VLAN in the "voice" role (and not in the edge port settings)

D. As the allowed trunk VLAN in the "voice" role (and not in the edge port settings)

Answer: D

Explanation:

When configuring 802.1X authentication on edge ports of an AOS-CX switch and assigning VoIP phones to a "voice" role, the correct approach is to configure VLAN 12 as the allowed trunk VLAN in the "voice" role. This setup ensures that traffic tagged for VLAN 12 is appropriately managed by the role applied to the VoIP phones. In AOS-CX switches, the role-based VLAN configuration allows for more granular control and ensures that the VoIP phones' traffic is handled correctly without altering the edge port settings, which typically operate with default settings for authentication.

Reference: Detailed configuration and role assignment practices for AOS-CX switches can be found in Aruba's configuration guides and documentation related to AOS-CX switch deployments.

Question: 2

You need to set up HPE Aruba Networking ClearPass Policy Manager (CPPM) to provide certificate-based authentication of 802.1X supplicants.

How should you upload the root CA certificate for the supplicants' certificates?

A. As a ClearPass Server certificate with the RADIUS/EAP usage

B. As a Trusted CA with the AD/LDAP usage

C. As a Trusted CA with the EAP usage

D. As a ClearPass Server certificate with the Database usage

Answer: C

Explanation:

To set up HPE Aruba Networking ClearPass Policy Manager (CPPM) for certificate-based authentication of 802.1X supplicants, you need to upload the root CA certificate as a Trusted CA with the EAP usage. This configuration allows the ClearPass server to validate the certificates presented by the supplicants during the 802.1X authentication process. By marking the certificate for EAP usage, ClearPass can properly authenticate the supplicant devices using the trusted certificate authority (CA) that issued their certificates.

Reference: Configuration guidelines and best practices for ClearPass Policy Manager are available in Aruba's ClearPass documentation, specifically detailing the steps for uploading and configuring root CA certificates for EAP-based authentication.

Question: 3

You have run an Active Endpoint Security Report on HPE Aruba Networking ClearPass. The report indicates that hundreds of endpoints have MAC addresses but

no known IP addresses.

What is one step for addressing this issue?

A. Set up network devices to implement RADIUS accounting to CPPM.

B. Add CPPM's IP address to the IP helper list on routing switches.

C. Set up switches to implement ARP inspection on client VLANs.

D. Configure CPPM as a Syslog destination on network devices.

Answer: B

Explanation:

When the Active Endpoint Security Report on HPE Aruba Networking ClearPass indicates that endpoints have MAC addresses but no known IP addresses, one effective step to address this issue is to add CPPM's (ClearPass Policy Manager) IP address to the IP helper list on routing switches. This configuration ensures that DHCP requests are forwarded to the ClearPass server, allowing it to track and report the IP addresses assigned to the endpoints. This helps ClearPass maintain an accurate mapping of MAC addresses to IP addresses, improving endpoint visibility and security management.

Reference: ClearPass configuration guides and best practices documentation outline the importance of integrating ClearPass with network infrastructure using IP helper addresses to ensure comprehensive endpoint visibility and management.

Question: 4

An admin has configured an AOS-CX switch with these settings:

port-access role employees

vlan access name employees

This switch is also configured with CPPM as its RADIUS server.

Which enforcement profile should you configure on CPPM to work with this configuration?

A. RADIUS Enforcement type with HPE-User-Role VSA set to "employees"

B. HPE Aruba Networking Downloadable Role Enforcement type with role name set to "employees"

C. HPE Aruba Networking Downloadable Role Enforcement type with gateway role name set to "employees"

D. RADIUS Enforcement type with Aruba-User-Role VSA set to "employees"

Answer: D

Explanation:

To ensure that the AOS-CX switch properly assigns the "employees" role when using CPPM (ClearPass Policy Manager) as the RADIUS server, you should configure a RADIUS Enforcement profile on CPPM with the Aruba-User-Role VSA (Vendor-Specific Attribute) set to "employees". This configuration ensures that when an endpoint authenticates, CPPM sends the appropriate role assignment to the AOS-CX switch, which then applies the corresponding policies and VLAN settings defined for the "employees" role.

Reference: Aruba's ClearPass documentation and AOS-CX configuration guides detail the integration and configuration of RADIUS enforcement profiles using Aruba-User-Role VSAs for role-based access control.

Question: 5

The security team needs you to show them information about MAC spoofing attempts detected by HPE Aruba Networking ClearPass Policy Manager (CPPM).

What should you do?

A. Export the Access Tracker records on CPPM as an XML file.

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

C. Integrate CPPM with ClearPass Device Insight (CPDI) and run a security report on CPDI.

D. Show the security team the CPPM Endpoint Profiler dashboard.

Answer: B

Explanation:

To show the security team information about MAC spoofing attempts detected by HPE Aruba Networking ClearPass Policy Manager (CPPM), you should use ClearPass Insight to run an Active Endpoint Security report. ClearPass Insight provides comprehensive reporting capabilities that include detailed information on security incidents, such as MAC spoofing attempts. By generating this report, you can provide the security team with a clear overview of the detected spoofing activities, including the endpoints involved and the context of the events.

Reference: The ClearPass documentation and Insight reporting guide offer detailed instructions on generating and interpreting Active Endpoint Security reports, which include data on MAC spoofing and other security incidents.

Question: 6

You need to set up an HPE Aruba Networking VIA solution for a customer who needs to support 2100 remote employees. The customer wants employees to

download their VIA connection profile from the VPNC. Only employees who authenticate with their domain credentials to HPE Aruba Networking ClearPass Policy

Manager (CPPM) should be able to download the profile. (A RADIUS server group for CPPM is already set up on the VPNC.)

How do you configure the VPNC to enforce that requirement?

A. Set up a VIA Authentication Profile that uses CPPM's server group; reference that profile in the VIA Web Authentication Profile.

B. Reference CPPM's server group in an AAA profile; then, apply that profile to the VPNC's Internetfacing ports.

C. Create a new VPN Authentication Profile and then reference CPPM's default server group in that profile.

D. Set up a VIA Authentication Profile that uses CPPM's server group; reference that profile in the VIA Connection Profile.

Answer: A

Explanation:

To configure the HPE Aruba Networking VIA solution for remote employees who need to download their VIA connection profile from the VPN Concentrator (VPNC) and ensure that only those who authenticate with their domain credentials through ClearPass Policy Manager (CPPM) can do so, you need to set up a VIA Authentication Profile. This profile should use the CPPM's RADIUS server group. Once the VIA Authentication Profile is created, you need to reference this profile in the VIA Web Authentication Profile. This configuration ensures that the authentication process requires employees to validate their credentials via CPPM before they can download the VIA connection profile.

Reference: Aruba's VIA deployment and configuration guides provide detailed steps on setting up authentication profiles and integrating ClearPass for secure profile distribution.

Question: 7

A company is using HPE Aruba Networking ClearPass Device Insight (CPDI) (the standalone application). You have identified a device, which is currently

classified as one type, but you want to classify it as a custom type. You also want to classify all devices with similar attributes as this type, both already-discovered

devices and new devices discovered later.

What should you do?

A. Create a user tag from the Generic Devices page, select the desired attributes for the tag, and save the tag.

B. In the device details, select reclassify, create a user rule based on its attributes, and choose "Save & Reclassify."

C. In the device details, select filter, create a user tag based on the device attributes, and save the tag.

D. Create a user rule from the Generic Devices page, select the desired attributes for the rule, and

choose "Save."

Answer: B

Explanation:

When using HPE Aruba Networking ClearPass Device Insight (CPDI) and you need to reclassify a device to a custom type and apply this classification to all devices with similar attributes, both already discovered and newly discovered, you should follow these steps:

1. Navigate to the device details in CPDI.
2. Select the option to reclassify the device.
3. Create a user rule based on the desired attributes of the device.
4. Choose the "Save & Reclassify" option.

This process ensures that the device is reclassified according to the new custom type and that the rule is applied to all existing and future devices with matching attributes, maintaining consistent classification across the network.

Reference: The ClearPass Device Insight user guide includes detailed instructions on device classification, rule creation, and managing device attributes to maintain accurate network visibility and security.

Question: 8

You are deploying a virtual Data Collector for use with HPE Aruba Networking ClearPass Device Insight (CPDI). You have identified VLAN 101 in the data center

as the VLAN to which the Data Collector should connect to receive its IP address and connect to HPE Aruba Networking Central.

Which Data Collector virtual ports should you tell the virtual admins to connect to VLAN 101?

A. The one with the lowest MAC address

B. The one with the highest port ID

C. The one with the highest MAC address

D. The one with the lowest port ID

Answer: D

Explanation:

When deploying a virtual Data Collector for HPE Aruba Networking ClearPass Device Insight (CPDI), it is essential to ensure that the correct virtual port is connected to the designated VLAN. In this case, VLAN 101 is used to receive the IP address and connect to Aruba Central. The best practice is to use the virtual port with the lowest port ID. This is typically the primary port used for management and network connectivity in virtual environments, ensuring proper network integration and communication.

Reference: Aruba's ClearPass Device Insight deployment guides and virtual appliance setup documentation provide detailed instructions on configuring network interfaces and VLAN assignments.

Question: 9

A company assigns a different block of VLAN IDs to each of its access layer AOS-CX switches. The switches run version 10.07. The IDs are used for standard

purposes, such as for employees, VoIP phones, and cameras. The company wants to apply 802.1X authentication to HPE Aruba Networking ClearPass Policy

Manager (CPPM) and then steer clients to the correct VLANs for local forwarding.

What can you do to simplify setting up this solution?

A. Assign consistent names to VLANs of the same type across the AOS-CX switches and have user-roles reference names.

B. Use the trunk allowed VLAN setting to assign multiple VLAN IDs to the same role.

C. Change the VLAN IDs across the AOS-CX switches so that they are consistent.

D. Avoid configuring the VLAN in the role; use trunk VLANs to assign multiple VLANs to the port instead.

Answer: A

Explanation:

To simplify the setup of 802.1X authentication with HPE Aruba Networking ClearPass Policy Manager (CPPM) and ensure clients are steered to the correct VLANs for local forwarding, you should assign consistent names to VLANs of the same type across the AOS-CX switches and have user-roles reference these names. This approach allows for a more straightforward configuration and management process, as the user roles can apply consistent policies based on VLAN names rather than specific IDs. It also helps in maintaining clarity and reducing errors in VLAN assignments across different switches.

Reference: Aruba's AOS-CX configuration guides and ClearPass integration documentation emphasize the importance of using consistent naming conventions and user-role configurations for efficient network management and security enforcement.

Question: 10

A company lacks visibility into the many different types of user and loT devices deployed in its internal network, making it hard for the security team to address

those devices.

Which HPE Aruba Networking solution should you recommend to resolve this issue?

A. HPE Aruba Networking ClearPass Device Insight (CPDI)

B. HPE Aruba Networking Network Analytics Engine (NAE)

C. HPE Aruba Networking Mobility Conductor

D. HPE Aruba Networking ClearPass OnBoard

Answer: A

Explanation:

For a company that lacks visibility into various types of user and IoT devices on its internal network, HPE Aruba Networking ClearPass Device Insight (CPDI) is the recommended solution. CPDI provides comprehensive visibility and profiling of all devices connected to the network. It uses machine learning and AI to identify and classify devices, offering detailed insights into their behavior and characteristics. This enhanced visibility enables the security team to effectively monitor and manage network devices, improving overall network security and compliance.

Reference: Aruba's documentation on ClearPass Device Insight outlines its capabilities in device discovery, profiling, and security posture assessment, making it ideal for environments with diverse and numerous network-connected devices.

Question: 11

A company is using HPE Aruba Networking ClearPass Device Insight (CPDI) (the standalone application). In the CPDI security settings, Security Analysis is On,

the Data Source is ClearPass Devices Insight, and Enable Posture Assessment is On. You see that device has a Risk Score of 90.

What can you know from this information?

A. The posture is unhealthy, and CPDI has also detected at least one vulnerability on the device.

B. The posture is unhealthy, but CPDI has not detected any vulnerabilities on the device.

C. The posture is healthy, but CPDI has detected multiple vulnerabilities on the device.

D. The posture is unknown, and CPDI has detected exactly four vulnerabilities on the device.

Answer: A

Explanation:

In HPE Aruba Networking ClearPass Device Insight (CPDI), a device with a Risk Score of 90 indicates that the posture is unhealthy, and CPDI has detected at least one vulnerability on the device. The risk score is a reflection of the device's security posture and detected vulnerabilities. A high risk score, such as 90, typically signifies significant security concerns,

including the presence of vulnerabilities that could be exploited, thereby categorizing the device as a high-risk asset within the network.

Reference: ClearPass Device Insight documentation and security settings guides explain how risk scores are calculated and interpreted, including the impact of posture assessment and vulnerability detection on overall device risk ratings.

Question: 12

You have set up a mirroring session between an AOS-CX switch and a management station, running Wireshark. You want to capture just the traffic sent in the

mirroring session, not the management station's other traffic.

What should you do?

A. Apply this capture filter: ip proto 47

B. Edit protocol preferences and enable ARUBA_ERM.

C. Edit protocol preferences and enable HPE_ERM.

D. Apply this capture filter: udp port 5555

Answer: D

Explanation:

To capture only the traffic sent in the mirroring session between an AOS-CX switch and a management station running Wireshark, you should apply a capture filter that isolates the specific traffic of interest. In this case, using the filter udp port 5555 will capture the traffic associated with the mirroring session. This is because AOS-CX switches typically use UDP port 5555 for mirrored traffic, ensuring that only the relevant mirrored packets are captured and excluding other traffic generated by the management station.

Reference: Aruba's AOS-CX documentation and network management guides detail the configuration and monitoring of traffic mirroring sessions, including the use of specific ports for mirrored traffic.

Question: 13

A company uses HPE Aruba Networking ClearPass Policy Manager (CPPM) as a TACACS+ server to authenticate managers on its AOS-CX switches. The

company wants CPPM to control which commands managers are allowed to enter. You see there is no field to enter these commands in ClearPass.

How do you start configuring the command list on CPPM?

A. Add the Shell service to the managers' TACACS+ enforcement profiles.

B. Edit the TACACS+ settings in the AOS-CX switches' network device entries.

C. Create an enforcement policy with the TACACS+ type.

D. Edit the settings for CPPM's default TACACS+ admin roles.

Answer: A

Explanation:

To control which commands managers are allowed to enter on AOS-CX switches using HPE Aruba Networking ClearPass Policy Manager (CPPM) as a TACACS+ server, you need to add the Shell service to the TACACS+ enforcement profiles for the managers. This service allows you to define and enforce specific command sets and access privileges for users authenticated via TACACS+. By configuring the Shell service in the enforcement profile, you can specify the commands that are permitted or denied for the managers, ensuring controlled and secure access to the switch's command-line interface.

Reference: Aruba's ClearPass Policy Manager documentation provides detailed instructions on setting up TACACS+ services, including configuring Shell profiles for command authorization and enforcement policies.

Question: 14

HPE Aruba Networking ClearPass Policy Manager (CPPM) uses a service to authenticate clients. You are now adding the Endpoints Repository as an

authorization source for the service, and you want to add rules to the service's policies that apply different access levels based, in part, on a client's device

category. You need to ensure that CPPM can apply the new correct access level after discovering new clients' categories.

What should you enable on the service?

A. The Posture Compliance option in the Service tab

B. The Profile Endpoints option in the Service tab

C. The Use cached Roles and Posture attributes from previous sessions option in the Enforcement tab

D. The Audit End-host option in the Service tab

Answer: B

Explanation:

To ensure that HPE Aruba Networking ClearPass Policy Manager (CPPM) can apply the correct access levels based on a client's device category after discovering new clients, you need to enable the "Profile Endpoints" option in the Service tab. This option allows CPPM to profile and categorize endpoints dynamically, ensuring that the appropriate access levels are applied based on the device's characteristics. Enabling this feature ensures that new devices are accurately profiled and that access policies can be enforced based on the updated device information.

Reference: Aruba ClearPass documentation and profiling guides detail the configuration and use of endpoint profiling to enhance access control and policy enforcement based on device categories.

Question: 15

A company has HPE Aruba Networking Central-managed APs. The company wants to block all clients connected through the APs from using YouTube.

Which steps should you take?

A. Deploy gateways and have the APs tunnel traffic to the gateways. Then, enable the gateway IDS/IPS engine.

B. Enable Client IPS at the "custom" level, and then specify the check for YouTube.

C. Enable WebCC on all client firewall roles. Then, create WebCC category rules that deny suspicious URLs.

D. Enable DPI. Then, create application rules to deny YouTube on the firewall roles.

Answer: D

Explanation:

To block all clients connected through HPE Aruba Networking Central-managed APs from accessing YouTube, you should enable DPI (Deep Packet Inspection) and then create application rules to deny YouTube on the firewall roles. DPI allows the network to inspect and classify traffic based on application signatures, making it possible to enforce application-specific policies. By creating rules that specifically block YouTube traffic, you can effectively prevent clients from accessing the service.

Reference: Aruba Central's documentation on firewall and application control provides detailed instructions on enabling DPI and creating application rules to manage and restrict access to specific applications such as YouTube.

Question: 16

What is one use case for implementing user-based tunneling (UBT) on AOS-CX switches?

A. Centralizing the distribution of wired traffic without requiring HPE Aruba Networking gateways

B. Tunneling traffic directly to a third-party firewall in a client data center

C. Adding 802.1X while continuing to use the existing VLAN and ACL structure in the Ethernet network

D. Applying enhanced security features such as deep packet inspection (DPI) to wired traffic

Answer: D

Explanation:

Implementing user-based tunneling (UBT) on AOS-CX switches is beneficial for applying enhanced security features such as deep packet inspection (DPI) to wired traffic. UBT allows the traffic from specific users or devices to be tunneled to a central controller or security appliance where advanced security policies, including DPI, can be applied. This approach ensures that even wired traffic benefits from the same level of security and inspection typically available for wireless

traffic, thus enhancing overall network security.

Reference: Aruba's documentation on UBT and AOS-CX configuration guides detail how to set up user-based tunneling and the benefits of applying advanced security features like DPI to tunneled traffic.

Question: 17

A company has HPE Aruba Networking APs running AOS-10 that connect to AOS-CX switches. The APs will:

. Authenticate as 802.1X supplicants to HPE Aruba Networking ClearPass Policy Manager (CPPM)

. Be assigned to the "APs" role on the switches

. Have their traffic forwarded locally

What information do you need to help you determine the VLAN settings for the "APs" role?

A. Whether the APs have static or DHCP-assigned IP addresses

B. Whether the switches are using local user-roles (LURs) or downloadable user-roles (DURs)

C. Whether the switches have established tunnels with an HPE Aruba Networking gateway

D. Whether the APs bridge or tunnel traffic on their SSIDs

Answer: D

Explanation:

To determine the VLAN settings for the "APs" role on AOS-CX switches, it is crucial to know whether the APs bridge or tunnel traffic on their SSIDs. If the APs are bridging traffic, the VLAN settings on the switch need to align with the VLANs used by the SSIDs. If the APs are tunneling traffic to a controller or gateway, the VLAN settings might differ as the traffic is encapsulated and forwarded through the tunnel. Understanding this aspect ensures that the VLAN configuration on the switches correctly supports the traffic forwarding method employed by the APs.

Reference: Aruba's AOS-10 and AOS-CX documentation provide guidance on VLAN configuration and traffic forwarding methods, highlighting the importance of aligning VLAN settings with the APs' traffic handling mode.

Question: 18

Your company wants to implement Tunneled EAP (TEAP).

How can you set up HPE Aruba Networking ClearPass Policy Manager (CPPM) to enforce certificatedbased authentication for clients using TEAP?

A. For the service using TEAP, set the authentication source to an internal database.

B. Select a service certificate when you specify TEAP as a service's authentication method.

C. Create an authentication method named "TEAP" with the type set to EAP-TLS.

D. Select an EAP-TLS-type authentication method for the TEAP method's inner method.

Answer: D

Explanation:

To set up HPE Aruba Networking ClearPass Policy Manager (CPPM) to enforce certificate-based authentication for clients using Tunneled EAP (TEAP), you need to select an EAP-TLS-type authentication method for TEAP's inner method. TEAP allows for a combination of certificate-based (EAP-TLS) and password-based (EAP-MSCHAPv2) authentication. By choosing EAP-TLS as the inner method, you ensure that the clients are authenticated using their certificates, thus enforcing

certificate-based authentication within the TEAP framework.

Reference: Aruba ClearPass documentation provides detailed steps for configuring TEAP and selecting appropriate inner authentication methods to ensure secure certificate-based client authentication.

Question: 19

Admins have recently turned on Wireless IDS/IPS infrastructure detection at the high level on HPE Aruba Networking APs. When you check WIDS events, you

see several RTS rate and CTS rate anomalies, which were triggered by neighboring APs.

What can you interpret from this event?

A. These neighboring APs are likely to be wireless clients that are inappropriately bridging their wired and wireless NICs; you should track down and remove them.

B. These neighboring APs might be hackers trying to launch a DoS, but are more likely operating normally; you should start by tuning the event thresholds.

C. These neighboring APs are actually rogue APs, and you should enable wireless tarpit containment on them.

D. These neighboring APs are actually rogue APs, and you should enable wireless de-authentication containment on them.

Answer: B

Explanation:

When Wireless IDS/IPS infrastructure detection reports RTS (Request to Send) and CTS (Clear to Send) rate anomalies triggered by neighboring APs, it is often an indication of unusual, but not necessarily malicious, behavior. These anomalies can be caused by neighboring APs operating normally but under specific conditions that trigger the alerts. Before assuming a security threat, it is recommended to tune the event thresholds to better match the environment and reduce false positives. This approach helps to distinguish between normal operations and potential DoS attacks.

Reference: Aruba's Wireless IDS/IPS configuration guides provide information on interpreting events, adjusting thresholds, and distinguishing between legitimate and malicious activities in a wireless network environment.

Question: 20

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. 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.

Reference: Aruba Central documentation and RAPIDS events management guides offer strategies for locating and responding to detected security threats, emphasizing the use of network tools and floorplans to effectively address potential vulnerabilities.

Question: 21

A company has a variety of HPE Aruba Networking solutions, including an HPE Aruba Networking infrastructure and HPE Aruba Networking ClearPass Policy

Manager (CPPM). The company passes traffic from the corporate LAN destined to the data center through a third-party SRX firewall. The company would like to further protect itself from internal threats.

What is one solution that you can recommend?

A. Have the third-party firewall send Syslogs to CPPM, which can work with network devices to lock internal attackers out of the network.

B. Use tunnel mode SSIDs and user-based tunneling (UBT) on AOS-CX switches to pass all internal traffic directly through the third-party firewall.

C. Add ClearPass Device Insight (CPDI) to the solution; integrate it with the third-party firewall to develop more complete device profiles.

D. Configure CPPM to poll the third-party firewall for a broad array of information about internal clients, such as profile and posture.

Answer: A

Explanation:

To further protect the company from internal threats, you can recommend having the third-party SRX firewall send Syslogs to HPE Aruba Networking ClearPass Policy Manager (CPPM). ClearPass can analyze these logs to detect potential security incidents and coordinate with network devices to respond to threats. By integrating Syslog data from the firewall, CPPM can identify malicious activities and take actions such as locking internal attackers out of the network or triggering specific security policies. This approach enhances the company's internal threat detection and response capabilities.

Reference: Aruba's ClearPass documentation on integrating with third-party security solutions and utilizing Syslog data for enhanced network security provides detailed guidance on setting up and using these features.

Question: 22

A company wants to apply a standard configuration to all AOS-CX switch ports and have the ports dynamically adjust

their configuration based on the identity of

the user or device that connects. They want to centralize configuration of the identity-based settings as much as possible.

What should you recommend?

A. Having HPE Aruba Networking ClearPass Policy Manager (CPPM) send standard RADIUS AVPs to customize port settings

B. Having switches pull port configurations dynamically from HPE Aruba Networking Activate

C. Having switches download user-roles from HPE Aruba Networking gateways

D. Having switches download user-roles from HPE Aruba Networking ClearPass Policy Manager (CPPM)

Answer: D

Explanation:

For a company that wants to apply a standard configuration to all AOS-CX switch ports and dynamically adjust their configuration based on the identity of the user or device that connects, the best approach is to have the switches download user-roles from HPE Aruba Networking ClearPass Policy Manager (CPPM). This method centralizes the configuration of identity-based settings in CPPM, allowing it to dynamically assign roles and policies to switch ports based on authentication and authorization results. This ensures consistent and secure network access control tailored to each user or device.

Reference: Aruba ClearPass and AOS-CX documentation provide comprehensive details on configuring user-roles, dynamic port configuration, and integrating ClearPass for centralized identitybased network management.

Question: 23

A company issues user certificates to domain computers using its Windows CA and the default user

certificate template. You have set up HPE Aruba Networking

ClearPass Policy Manager (CPPM) to authenticate 802.1X clients with those certificates. However, during tests, you receive an error that authorization has failed

because the usernames do not exist in the authentication source.

What is one way to fix this issue and enable clients to successfully authenticate with certificates?

A. Configure rules to strip the domain name from the username.

B. Change the authentication method list to include both PEAP MSCHAPv2 and EAP-TLS.

C. Add the ClearPass Onboard local repository to the authentication source list.

D. Remove EAP-TLS from the authentication method list and add TEAP there instead.

Answer: A

Explanation:

To fix the issue where authorization fails because the usernames do not exist in the authentication source, you can configure rules in HPE Aruba Networking ClearPass Policy Manager (CPPM) to strip the domain name from the username. When certificates are issued by a Windows CA, the username in the certificate often includes the domain (e.g., user@domain.com). ClearPass might not be able to find this format in the authentication source. By stripping the domain name, you ensure that ClearPass searches for just the username (e.g., user) in the authentication source, allowing successful authentication.

Reference: ClearPass configuration guides and documentation on certificate-based authentication detail the process of modifying and normalizing usernames to ensure successful authentication against authentication sources.

Question: 24

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

Which guideline should you follow?

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.

Reference: Aruba ClearPass documentation provides guidelines on configuring enforcement policies and using posture attributes effectively, including the importance of caching for maintaining posture information across sessions.

Question: 25

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 the company has rare Internet of Things (IoT) devices

B. Whether some devices are incapable of captive portal or 802.1X authentication

C. Whether the company has devices that use PXE boot

D. Whether some devices are running legacy operating systems

Answer: C

Explanation:

When you have created a rule in a ClearPass Policy Manager (CPPM) service's enforcement policy to quarantine devices with endpoint conflicts, it is important to consider whether the company has devices that use PXE boot. PXE booting

devices can create conflicts in the profiler because they may temporarily have different network attributes (e.g., MAC address or IP address) before fully booting and obtaining their final configuration. Understanding whether PXE boot is in use can help determine if profiler parameters need to be adjusted to ignore such temporary conflicts, ensuring that devices are not incorrectly quarantined.

Reference: ClearPass profiler configuration documentation and best practices include considerations for handling network devices with dynamic or temporary configurations, such as those using PXE boot.

Question: 26

A company has HPE Aruba Networking APs, which authenticate users to HPE Aruba Networking ClearPass Policy Manager (CPPM).

What does HPE Aruba Networking recommend as the preferred method for assigning clients to a role on the AOS firewall?

A. Configure CPPM to assign the role using a RADIUS enforcement profile with a RADIUS:IETF Username attribute.

B. Configure CPPM to assign the role using a RADIUS enforcement profile with an Aruba-User-Role VSA.

C. OCreate server rules on the APs to assign clients to roles based on RADIUS IETF attributes returned by CPPM.

D. Create user rules on the APs to assign clients to roles based on a variety of criteria.

Answer: B

Explanation:

The preferred method for assigning clients to a role on the AOS firewall is to configure HPE Aruba Networking ClearPass Policy Manager (CPPM) to assign the role using a RADIUS enforcement profile with an Aruba-User-Role VSA (Vendor-Specific Attribute). This method allows ClearPass to dynamically assign the appropriate user roles to clients during the authentication process, ensuring that role-based access policies are consistently enforced across the network.

Reference: Aruba ClearPass documentation and RADIUS configuration guides provide detailed instructions on setting up RADIUS enforcement profiles and using the Aruba-User-Role VSA for role assignment.

Question: 27

A security team needs to track a device's communication patterns and identify patterns such as how many destinations the device is accessing.

Which Aruba solution can show this information at a glance?

A. HPE Aruba Networking ClearPass Insight Endpoints and Network Dashboards

B. HPE Aruba Networking ClearPass Policy Manager (CPPM) live monitoring Access Tracker

C. HPE Aruba Networking ClearPass Device Insight (CPDI) under a device's network activity

D. AOS-CX Analytics Dashboard using the system-installed NAE agent

Answer: C

Explanation:

HPE Aruba Networking ClearPass Device Insight (CPDI) can show detailed information about a device's communication patterns, including how many destinations the device is accessing. CPDI provides comprehensive visibility into the behavior and activity of devices on the network, allowing the security team to track and analyze communication patterns at a glance. This information is critical for identifying anomalies and potential security threats.

Reference: ClearPass Device Insight documentation and network activity monitoring guides offer insights into tracking and analyzing device communication patterns using CPDI's capabilities.

Question: 28

A company uses HPE Aruba Networking ClearPass Policy Manager (CPPM) as a TACACS+ server to authenticate managers on its AOS-CX switches. You want

to assign managers to groups on the AOS-CX switch by name.

How do you configure this setting in a CPPM TACACS+ enforcement profile?

A. Add the Shell service and set autocmd to the group name.

B. Add the Shell service and set priv-lvl to the group name.

C. Add the Aruba:Common service and set Aruba-Admin-Role to the group name.

D. Add the Aruba:Common service and set Aruba-Priv-Admin-User to the group name.

Answer: C

Explanation:

To assign managers to groups on the AOS-CX switch by name using HPE Aruba Networking ClearPass Policy Manager (CPPM) as a TACACS+ server, you should add the Aruba service to the TACACS+ enforcement profile and set the Aruba-Admin-Role to the group name. This configuration ensures that the appropriate administrative roles are assigned to managers based on their group membership, allowing for role-based access control on the AOS-CX switches.

Reference: ClearPass TACACS+ configuration guides and AOS-CX switch management documentation provide details on setting up enforcement profiles and using the Aruba-Admin-Role attribute for role assignment.

Question: 29

What is one use case that companies can fulfill using HPE Aruba Networking ClearPass Policy Manager's (CPPM's) Device Profiler?

A. OIdentifying device security vulnerabilities by CVE ID and receiving remediation recommendations

B. Leveraging artificial intelligence to more accurately identify Internet of Things (IoT) devices

C. Quarantining devices that do not have the required antivirus software installed on them

D. Assigning different AOS firewall roles to users on computers and the same users on smartphones

Answer: B

Explanation:

One use case that companies can fulfill using HPE Aruba Networking ClearPass Policy Manager's (CPPM's) Device Profiler

is leveraging artificial intelligence to more accurately identify Internet of Things (IoT) devices. ClearPass Device Profiler uses AI and machine learning to analyze network traffic and device behavior, providing detailed and accurate identification of IoT devices on the network. This helps in managing and securing diverse and numerous IoT devices by ensuring they are correctly profiled and assigned appropriate access policies.

Reference: Aruba ClearPass documentation highlights the use of AI and machine learning in device profiling to enhance the identification and management of IoT devices.

Question: 30

A company needs to enforce 802.1X authentication for its Windows domain computers to HPE Aruba Networking ClearPass Policy Manager (CPPM). The company needs the computers to authenticate as both machines and users in the same session.

Which authentication method should you set up on CPPM?

A. TEAP

B. PEAP MSCHAPv2

C. EAP-TTLS

D. EAP-TLS

Answer: A

Explanation:

To enforce 802.1X authentication for Windows domain computers to HPE Aruba Networking ClearPass Policy Manager (CPPM) and have the computers authenticate as both machines and users in the same session, you should set up TEAP (Tunneled EAP) as the authentication method. TEAP supports both machine and user authentication within a single 802.1X session, making it suitable for scenarios where both types of authentication are required simultaneously.

Reference: Aruba ClearPass configuration guides provide detailed instructions on setting up TEAP for environments requiring combined machine and user authentication.

Question: 31

A company is implementing HPE Aruba Networking Wireless IDS/IPS (WIDS/WIPS) on its AOS-10 APs, which are

managed in HPE Aruba Networking Central.

What is one requirement for enabling detection of rogue APs?

A. Each VLAN in the network assigned on at least one AP's or AM's port

B. A Foundation with Security license for each of the APs

C. One AM deployed for every one AP deployed

D. A manual radio profile that enables non-regulatory channels

Answer: B

Explanation:

To enable the detection of rogue APs with HPE Aruba Networking Wireless IDS/IPS (WIDS/WIPS) on AOS-10 APs managed in HPE Aruba Networking Central, each AP must have a Foundation with Security license. This license enables advanced security features, including rogue AP detection, which is crucial for maintaining a secure wireless environment and protecting against unauthorized access points.

Reference: Aruba's licensing documentation and WIDS/WIPS setup guides specify the need for appropriate licenses to activate security features such as rogue AP detection.

Question: 32

A company uses HPE Aruba Networking ClearPass Device Insight (CPDI) (the standalone application option). In the details for a generic device cluster, you see a

recommendation for "Windows 8/10" with 70% accuracy.

What does this mean?

A. CPDI has detected that these devices match about 70% of the system rule for defining "Windows 8/10" devices.

B. CPDI has matched these devices against several, conflicting system rules. 70% of those rules are for "Windows

8/10" devices.

C. CPDI has grouped this cluster with similar classified devices. 70% of those classified devices are "Windows 8/10."

D. CPDI has used MAC OUI to group these devices together. The average device's MAC address matches 70% of the "Windows 8/10" OUI.

Answer: A

Explanation:

When HPE Aruba Networking ClearPass Device Insight (CPDI) shows a recommendation for "Windows 8/10" with 70% accuracy for a generic device cluster, it means that CPDI has detected that

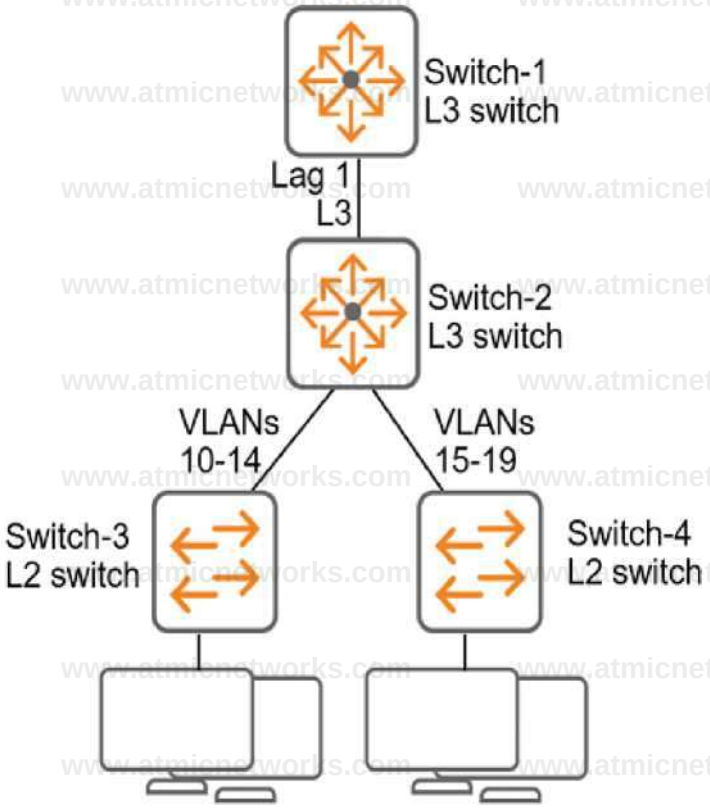
these devices match about 70% of the system rule criteria for defining "Windows 8/10" devices. This percentage indicates the confidence level based on the observed characteristics and behavior of the devices, helping administrators understand the likelihood that these devices are indeed running Windows 8 or 10.

Reference: ClearPass Device Insight documentation provides details on how device classification and accuracy percentages are determined, explaining the matching process against system rules.

Question: 33

Refer to the exhibit.

Refer to the exhibit.



All of the switches in the exhibit are AOS-CX switches.

What is the preferred configuration on Switch-2 for preventing rogue OSPF routers in this network?

A. Disable OSPF entirely on VLANs 10-19.

B. Configure OSPF authentication on VLANs 10-19 in password mode.

C. Configure OSPF authentication on Lag 1 in MD5 mode.

D. Configure passive-interface as the OSPF default and disable OSPF passive on Lag 1.

Answer: C

Explanation:

To prevent rogue OSPF routers in the network shown in the exhibit, the preferred configuration on Switch-2 is to configure OSPF authentication on Lag 1 in MD5 mode. This setup enhances security by ensuring that only routers with the correct MD5 authentication credentials can participate in the OSPF routing process. This method protects the OSPF sessions against unauthorized devices that might attempt to introduce rogue routing information into the network.

1. OSPF Authentication: Implementing MD5 authentication on Lag 1 ensures that OSPF updates are secured with a cryptographic hash. This prevents unauthorized OSPF routers from establishing peering sessions and injecting potentially malicious routing information.

2. Secure Communication: MD5 authentication provides a higher level of security compared to simple password authentication, as it uses a more robust hashing algorithm.

3. Applicability: Lag 1 is the primary link between Switch-1 and Switch-2, and securing this link helps protect the integrity of the OSPF routing domain.

Reference: Aruba's AOS-CX switch documentation and OSPF configuration guides detail how to set up MD5 authentication for OSPF to enhance network security against rogue devices.

Question: 34

What is a use case for the HPE Aruba Networking ClearPass OnGuard dissolvable agent?

A. Continuously monitoring Windows domain clients for compliance

B. Implementing a one-time compliance scan

C. Auto-remediating posture issues on clients

D. Periodically scanning Linux clients for security issues

Answer: B

Explanation:

The use case for the HPE Aruba Networking ClearPass OnGuard dissolvable agent is implementing a one-time compliance scan. The dissolvable agent is designed to perform a compliance check without requiring a permanent installation on the client device. This is ideal for environments where a quick, temporary assessment of the device's security posture is needed without the overhead of a persistent agent.

1. Dissolvable Agent: The dissolvable agent is downloaded and executed on the client device for a single session, performing the necessary compliance checks before being removed automatically.

2. One-time Compliance Scan: This method is particularly useful for guest or unmanaged devices where a temporary compliance scan is sufficient to ensure security standards are met.

3. Minimal Impact: Since the agent does not persist on the client device, it minimizes the impact on the user's

system and does not require ongoing maintenance or updates.

Reference: ClearPass OnGuard documentation details the capabilities and use cases for the dissolvable agent, emphasizing its role in one-time compliance assessments.

Question: 35

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:

Applying a time range to a firewall rule on an AOS device fulfills the use case of enforcing the rule only during the specified time range. This allows administrators to control when specific firewall rules are active, which can be useful for implementing policies that only need to be in effect during certain hours, such as blocking or allowing access to specific resources outside of business hours.

1. Time-Based Enforcement: The firewall rule will be active only during the specified time range, ensuring that the rule's policies are enforced only when needed.
2. Use Case: This feature is useful for scenarios like limiting access to certain applications or websites during working hours, or enabling enhanced security measures during off-hours.
3. Flexibility: Provides flexibility in security policy management by allowing dynamic adjustment of rules based on time schedules.

Reference: Aruba's AOS device documentation and firewall rule configuration guides detail how to apply time ranges to firewall rules for time-based policy enforcement.

Question: 36

A company wants HPE Aruba Networking ClearPass Policy Manager (CPPM) to respond to Syslog messages from its Palo Alto Next Generation Firewall (NGFW)

by quarantining clients involved in security incidents.

Which step must you complete to enable CPPM to process the Syslogs properly?

A. Configure the Palo Alto as a context server on CPPM.

B. Install a Palo Alto Extension through ClearPass Guest.

C. Enable Insight and ingress event processing on the CPPM server.

D. Configure CPPM to trust the root CA certificate for the NGFW.

Answer: A

Explanation:

To enable HPE Aruba Networking ClearPass Policy Manager (CPPM) to process Syslog messages from a Palo Alto Next Generation Firewall (NGFW) and quarantine clients involved in security incidents, you need to configure the Palo Alto as a context server on CPPM. This setup allows CPPM to receive and understand the context of the Syslog messages sent by the Palo Alto NGFW, enabling it to take appropriate actions such as quarantining clients.

1. Context Server Configuration: Configuring the Palo Alto NGFW as a context server in CPPM ensures that CPPM can process and respond to Syslog messages effectively.
2. Security Incident Response: By understanding the context of the Syslog messages, CPPM can automatically trigger actions like client quarantine based on security incidents detected by the NGFW.
3. Integration: This integration enhances the overall security posture by enabling coordinated responses between the firewall and CPPM.

Reference: ClearPass integration guides and context server configuration documentation provide detailed steps on setting up and utilizing context servers for security incident management.

Question: 37

A company is implementing a client-to-site VPN based on tunnel-mode IPsec.

Which devices are responsible for the IPsec encapsulation?

A. Gateways at the remote clients' locations and devices accessed by the clients at the main site

B. The remote clients and devices accessed by the clients at the main site

C. The remote clients and a gateway at the main site

D. Gateways at the remote clients' locations and a gateway at the main site

Answer: C

Explanation:

In a client-to-site VPN based on tunnel-mode IPsec, the remote clients and a gateway at the main site are responsible for the IPsec encapsulation. The remote clients initiate the VPN connection and encapsulate their traffic in IPsec, which is then decapsulated by the gateway at the main site.

1. IPsec Encapsulation: The remote clients encapsulate their traffic using IPsec protocols before sending it over the internet to the main site.

2. Gateway Role: The gateway at the main site receives the encapsulated traffic, decapsulates it, and forwards it to the internal network. Similarly, traffic from the main site to the remote clients is encapsulated by the gateway and decapsulated by the clients.

3. Security: This setup ensures that data is securely transmitted between the remote clients and the main site, protecting it from eavesdropping and tampering.

Reference: Aruba and general IPsec VPN configuration guides provide detailed information on setting up client-to-site VPNs, highlighting the roles of remote clients and gateways in IPsec encapsulation.

Question: 38

You are setting up an HPE Aruba Networking VIA solution for a company. You need to configure access control policies for applications and resources that remote

clients can access when connected to the VPN.

Where on the VPNC should you configure these policies?

A. In the tunneled network settings within the VIA Connection Profile

B. In the cloud security settings using IPsec maps

C. In the roles to which VIA clients are assigned after IKE authentication

D. In the roles to which VIA clients are assigned after VIA Web authentication

Answer: C

Explanation:

To configure access control policies for applications and resources that remote clients can access when connected to the VPN, you should configure these policies in the roles to which VIA clients are assigned after IKE (Internet Key Exchange) authentication on the VPNC. These roles define the permissions and access controls for the clients once they are authenticated, ensuring that they can only access the applications and resources allowed by their assigned roles.

1. IKE Authentication: After IKE authentication, clients are assigned specific roles that determine their access privileges.

2. Role-Based Access Control: By configuring access control policies within these roles, you can granularly control what resources and applications the remote clients can access over the VPN.

3. Security: This method ensures that access is managed securely and dynamically based on the role assigned to each client after successful authentication.

Reference: Aruba's VPN and VIA deployment guides provide detailed instructions on configuring roles and access control policies for remote VPN clients.

Question: 39

A company has HPE Aruba Networking APs running AOS-10 and managed by HPE Aruba Networking Central. The company also has AOS-CX switches. The

security team wants you to capture traffic from a particular wireless client. You should capture this client's traffic over a 15 minute time period and then send the traffic to them in a PCAP file.

What should you do?

A. Go to the client's AP in HPE Aruba Networking Central. Use the "Security" page to run a packet capture.

B. Access the CLI for the client's AP. Set up a mirroring session between its radio and a management station running Wireshark.

C. Access the CLI for the client's AP's switch. Set up a mirroring session between the AP's port and a management station running Wireshark.

D. Go to that client in HPE Aruba Networking Central. Use the "Live Events" page to run a packet capture.

Answer: A

Explanation:

To capture traffic from a particular wireless client for a 15-minute period and then send the traffic in a PCAP file, you should go to the client's AP in HPE Aruba Networking Central and use the "Security" page to run a packet capture. This method allows you to directly capture the client's traffic from the AP managing the wireless connection, ensuring that you gather the relevant traffic data for analysis.

1. Centralized Management: HPE Aruba Networking Central provides a centralized interface for managing and monitoring APs, making it easy to initiate packet captures.
2. Security Page: The "Security" page in Aruba Central includes tools for running packet captures, allowing you to specify the duration and other parameters.
3. Ease of Use: This approach simplifies the process by using the built-in features of Aruba Central, avoiding the need for complex CLI commands or additional hardware.

Reference: Aruba Central's documentation and user guides detail the steps for performing packet captures through the Central interface, including capturing traffic from specific clients and generating PCAP files for analysis.

Question: 40

Assume that an AOS-CX switch is already implementing DHCP snooping and ARP inspection successfully on several VLANs.

What should you do to help minimize disruption time if the switch reboots?

A. Configure the switch to act as an ARP proxy.

B. Create static IP-to-MAC bindings for the DHCP and DNS servers.

C. Save the IP-to-MAC bindings to external storage.

D. Configure the IP helper address on this switch, rather than a core routing switch.

Answer: C

Explanation:

To minimize disruption time if an AOS-CX switch reboots while implementing DHCP snooping and ARP inspection, you should save the IP-to-MAC bindings to external storage. This ensures that the DHCP snooping and ARP inspection tables, which are crucial for preventing spoofing attacks, are preserved across reboots. When the switch restarts, it can reload these bindings from the external storage, thereby maintaining network security and reducing the downtime associated with rebuilding these tables.

1. Preserving Bindings: Saving IP-to-MAC bindings to external storage ensures that these critical security tables are not lost during a reboot, maintaining network integrity.
2. Security Continuity: This practice helps to quickly restore security features like DHCP snooping and ARP inspection, minimizing the window of vulnerability.
3. Operational Efficiency: By preserving these bindings, the switch can resume normal operations faster, reducing disruption to network services.

Reference: Aruba's AOS-CX configuration guides and best practices for DHCP snooping and ARP inspection detail the importance of saving IP-to-MAC bindings for maintaining network security across reboots.

Question: 41

You need to create a rule in an HPE Aruba Networking ClearPass Policy Manager (CPPM) role mapping policy that references a ClearPass Device Insight Tag.

Which Type (namespace) should you specify for the rule?

A. Application

B. Tips

C. Device

D. Endpoint

Answer: D

Explanation:

When creating a rule in an HPE Aruba Networking ClearPass Policy Manager (CPPM) role mapping policy that references a ClearPass Device Insight Tag, you should specify the "Endpoint" Type (namespace) for the rule. This ensures that the policy can properly reference and utilize the tags assigned to endpoints by ClearPass Device Insight for making role mapping decisions.

1. Endpoint Tags: ClearPass Device Insight assigns tags to endpoints based on their characteristics and behaviors. These tags are stored in the "Endpoint" namespace.
2. Role Mapping: By referencing the "Endpoint" type, the rule can accurately match endpoints with the specified tags and apply the appropriate role mappings based on the device's profile.
3. Policy Consistency: Ensuring that the correct namespace is used maintains consistency and accuracy in role assignment policies.

Reference: ClearPass documentation and role mapping policy guides provide details on using Device Insight tags and the appropriate namespaces for creating effective policy rules.

Question: 42

You are using OpenSSL to obtain a certificate signed by a Certification Authority (CA). You have entered this command:

openssl req -new -out file1.pem -newkey rsa:3072 -keyout file2.pem

Enter PEM pass phrase: **********

Verifying - Enter PEM pass phrase: **********

Country Name (2 letter code) [AU]:US

State or Province Name (full name) [Some-State]:California

Locality Name (eg, city) []:Sunnyvale

Organization Name (eg, company) [Internet Widgits Pty Ltd]:example.com

Organizational Unit Name (eg, section) []:Infrastructure

Common Name (e.g. server FQDN or YOUR name) []:radius.example.com

What is one guideline for continuing to obtain a certificate?

A. You should use a third-party tool to encrypt file2.pem before sending it and file1.pem to the CA.

B. You should concatenate file1.pem and file2.pem into a single file, and submit that to the desired CA to sign.

C. You should submit file1.pem, but not file2.pem, to the desired CA to sign.

D. You should submit file2.pem, but not file1.pem, to the desired CA to sign.

Answer: C

Explanation:

When using OpenSSL to obtain a certificate signed by a Certification Authority (CA), you should submit the Certificate Signing Request (CSR) file, which is file1.pem, to the CA. The CSR contains the information about the entity requesting the certificate and the public key, but not the private key, which is in file2.pem. The CA uses the information in the CSR to create and sign the certificate.

1. CSR Submission: The CSR (file1.pem) includes the public key and the entity information required by the CA to issue a certificate.
2. Private Key Security: The private key (file2.pem) should never be sent to the CA or shared; it remains securely stored on the requestor's server.
3. Certificate Issuance: After the CA signs the CSR, the resulting certificate can be used with the private key to establish secure communications.

Reference: OpenSSL documentation and best practices for obtaining and managing certificates emphasize the importance of keeping the private key secure and only submitting the CSR to the CA.

Question: 43

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: C

Explanation:

To integrate HPE Aruba Networking ClearPass Policy Manager (CPPM) with HPE Aruba Networking ClearPass Device Insight (CPDI), one of the necessary tasks is to enable Insight in the CPPM server configuration settings. This configuration allows CPPM to communicate and share data with CPDI, facilitating the integration and enabling enhanced device profiling and policy enforcement capabilities.

1. Insight Enablement: Enabling Insight on the CPPM server allows it to leverage the data and capabilities of CPDI, integrating device profiling information into policy decisions.
2. Data Sharing: This integration ensures that CPPM can receive and use detailed device information from CPDI to make more informed policy enforcement decisions.
3. Configuration: Properly configuring the server settings to enable Insight ensures seamless communication and data flow between CPPM and CPDI.

Reference: Aruba ClearPass integration guides provide detailed instructions on enabling Insight and configuring the necessary settings for effective integration between CPPM and CPDI.

Question: 44

You have installed an HPE Aruba Networking Network Analytic Engine (NAE) script on an AOS-CX switch to monitor a particular function.

Which additional step must you complete to start the monitoring?

A. Reboot the switch.

B. Enable NAE, which is disabled by default.

C. Edit the script to define monitor parameters.

D. Create an agent from the script.

Answer: D

Explanation:

After installing an HPE Aruba Networking Network Analytic Engine (NAE) script on an AOS-CX switch, the additional step required to start the monitoring is to create an agent from the script. The agent is responsible for executing the script and collecting the monitoring data as defined by the script parameters.

1. Script Installation: Installing the script provides the logic and parameters for monitoring.
2. Agent Creation: Creating an agent from the script activates the monitoring process, allowing the NAE to begin tracking the specified function.
3. Operational Step: This step ensures that the monitoring logic is applied and the data collection starts as per the script's configuration.

Reference: Aruba AOS-CX documentation and Network Analytics Engine guides outline the process of script installation and the necessity of creating an agent to activate monitoring.

Question: 45

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:

To ensure that HPE Aruba Networking ClearPass Policy Manager (CPPM) applies tag-based rules to a client immediately after learning the client has that tag, verify that both 802.1X services have the "Profile Endpoints" option enabled and an appropriate Change of Authorization (CoA) profile selected in the Profiler tab. This setup ensures that when a device is profiled and tagged, CPPM can immediately enforce the updated policies through CoA.

1. Profile Endpoints: Enabling this option ensures that endpoint profiling is active, allowing CPPM to gather and use device information dynamically.

2. CoA Profile: Selecting an appropriate CoA profile ensures that CPPM can push policy changes immediately to the network devices, applying the new rules without delay.

3. Real-Time Enforcement: This configuration allows for the immediate application of new tags and associated policies, ensuring compliance with security requirements.

Reference: ClearPass documentation on endpoint profiling and CoA settings provides detailed steps for configuring these options to enable dynamic and immediate policy enforcement based on device profiling.

Question: 46

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: A

Explanation:

To support the requirement for HPE Aruba Networking ClearPass Policy Manager (CPPM) to have HTTP User-Agent strings for profiling devices, you should add the CPPM server's IP address to the IP helper list in all client VLANs on routing switches. This configuration ensures that DHCP requests and other relevant client traffic are forwarded to CPPM, allowing it to capture HTTP User-Agent strings and use them for device profiling.

1. IP Helper Configuration: Adding CPPM to the IP helper list ensures that the switch forwards DHCP and other client traffic to CPPM, enabling it to gather necessary information for profiling.
2. User-Agent Strings: By receiving client traffic, CPPM can analyze HTTP headers and capture UserAgent strings, which provide valuable information about the client's device and browser.
3. Profiling Support: This approach supports the comprehensive profiling of devices, allowing CPPM to apply appropriate policies based on detailed device information.

Reference: Aruba ClearPass and AOS-CX switch configuration guides detail the process of setting up IP helper addresses and the benefits of forwarding client traffic to CPPM for enhanced profiling and policy enforcement.

Question: 47

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: A

Explanation:

Running periodic subnet scans on devices from HPE Aruba Networking ClearPass Policy Manager (CPPM) can be used to gather DHCP fingerprints, which help determine a client's device category and operating system. DHCP fingerprints are unique patterns in DHCP request packets that provide valuable information about the device type and OS, assisting in device profiling and policy enforcement.

1. DHCP Fingerprinting: This technique captures specific details from DHCP packets to identify the type and operating system of a device.
2. Device Profiling: By running subnet scans, CPPM can continuously update its device database with accurate profiles, ensuring that policies are applied correctly based on the device type.
3. Network Visibility: Regular scanning helps maintain up-to-date visibility of all devices on the network, improving security and management.

Reference: ClearPass documentation on device profiling and network visibility outlines the use of DHCP fingerprints for identifying and categorizing devices, emphasizing the importance of periodic subnet scans for maintaining accurate profiles.

Question: 48

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?

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.

Reference: ClearPass documentation on CoA settings and best practices provides guidelines on tuning CoA delays to ensure accurate and timely application of updated profiles.

Question: 49

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:

When enabling Wireless IDS/IPS infrastructure and client detection at a high level on HPE Aruba Networking APs without enabling prevention settings, HPE Aruba Networking recommends configuring detection at a custom level and adjusting settings to minimize false positives. This approach allows for effective monitoring while reducing the risk of unnecessary alerts and maintaining the accuracy of detections.

1. Custom Level Configuration: By customizing the detection settings, you can tailor the system to your specific environment, ensuring that only relevant threats are detected and reducing false positives.

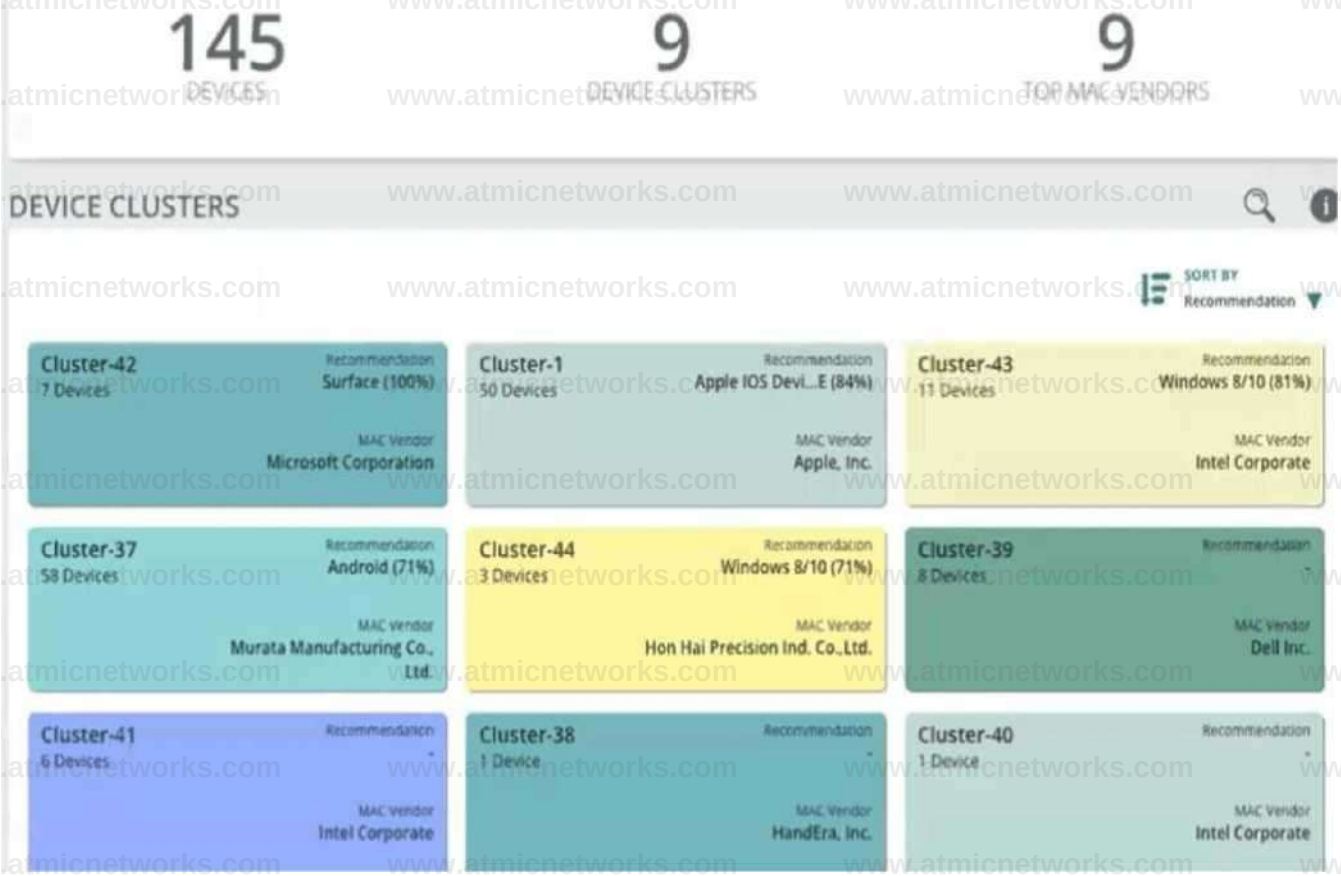
2. False Positive Reduction: Disabling or tuning settings that are likely to produce false positives helps in maintaining the reliability of the detection system and prevents alert fatigue.

3. Focused Detection: Custom configuration ensures that the IDS/IPS focuses on critical detections, improving overall security posture.

Reference: Aruba's Wireless IDS/IPS configuration guides and best practices emphasize the importance of customizing detection settings to balance security needs with operational efficiency, particularly when prevention features are not enabled.

Question: 50

Refer to Exhibit.



A company is using HPE Aruba Networking ClearPass Device Insight (CPDI) (the standalone application). In the CPDI interface, you go to the Generic Devices

page and see the view shown in the exhibit.

What correctly describes what you see?

A. Each cluster is a group of unclassified devices that CPDI's machine learning has discovered to have similar attributes.

B. Each cluster is a group of devices that match one of the tags configured by admins.

C. Each cluster is all the devices that have been assigned to the same category by one of CPDI's built- in system rules.

D. Each cluster is a group of devices that have been classified with user rules, but for which CPDI offers different recommendations.

Answer: A

Explanation:

In HPE Aruba Networking ClearPass Device Insight (CPDI), the clusters shown in the exhibit represent groups of unclassified devices that CPDI's machine learning algorithms have identified as having similar attributes. These clusters are formed based on observed characteristics and behaviors of the devices, helping administrators to categorize and manage devices more effectively.

1. Machine Learning: CPDI uses machine learning to analyze device attributes and group them into clusters based on similarities.
2. Unclassified Devices: These clusters typically represent devices that have not yet been explicitly classified by admins but share common attributes that suggest they belong to the same category.
3. Management: This clustering helps in simplifying the process of managing and applying policies to groups of similar devices.

Reference: ClearPass Device Insight documentation on device clustering and machine learning provides detailed information on how devices are grouped into clusters based on observed attributes and behaviors.

Question: 51

A company has AOS-CX switches and HPE Aruba Networking ClearPass Policy Manager (CPPM). The company wants switches to implement 802.1X

authentication to CPPM and download user roles.

What is one task that you must complete on the switches to support this use case?

A. Specify CPPM as the RADIUS server with the exact CN in CPPM's HTTPS certificate.

B. Install the root CA certificate for CPPM's RADIUS certificate in a TA profile on the switches.

C. Configure empty user-roles with names that match enforcement profile names on CPPM.

D. Specify a ClearPass username and password that match the name and RADIUS secret in a CPPM network device entry.

Answer: B

Explanation:

To support 802.1X authentication and download user roles from HPE Aruba Networking ClearPass Policy Manager (CPPM) on AOS-CX switches, you must install the root CA certificate for CPPM's RADIUS certificate in a Trust Anchor (TA)

profile on the switches. This ensures that the switches trust the RADIUS server certificate presented by CPPM during the authentication process.

1. Root CA Certificate: Installing the root CA certificate ensures that the switch can verify the authenticity of the RADIUS server certificate provided by CPPM.
2. Trust Anchor Profile: The TA profile on the switch holds the root CA certificate, establishing a trust relationship between the switch and the CPPM RADIUS server.
3. Secure Authentication: This setup is essential for securing the 802.1X authentication process and enabling the download of user roles.

Reference: AOS-CX switch configuration guides and ClearPass integration documentation detail the steps for installing root CA certificates and configuring trust anchor profiles to enable secure RADIUS authentication and role-based access control.

Question: 52

What is a benefit of Online Certificate Status Protocol (OCSP)?

A. It lets a device query whether a single certificate is revoked or not.

B. It lets a device dynamically renew its certificate before the certificate expires.

C. It lets a device download all the serial numbers for certificates revoked by a CA at once.

D. It lets a device determine whether to trust a certificate without needing any root certificates installed.

Answer: A

Explanation:

The benefit of the Online Certificate Status Protocol (OCSP) is that it allows a device to query whether a single certificate is revoked or not. OCSP provides a real-time mechanism for checking the revocation status of an individual certificate, enabling devices to verify the validity of certificates quickly and efficiently.

1. Certificate Status Query: OCSP enables devices to send a query to an OCSP responder to check the revocation status of a specific certificate.

2. Real-Time Verification: This protocol offers real-time responses, ensuring that the most up-to-date status of the certificate is obtained.

3. Efficiency: OCSP is more efficient than downloading an entire Certificate Revocation List (CRL), as it only queries the status of one certificate at a time.

Reference: Documentation on certificate management and OCSP describes how OCSP works and its advantages in providing real-time certificate status checks compared to traditional CRLs.

Question: 53

Refer to the exhibit.

Refer to the exhibit.

(Note that the HPE Aruba Networking Central interface shown here might look slightly different from what you see in your HPE Aruba Networking Central interface as versions change; however, similar concepts continue to apply.)

An HPE Aruba Networking 9x00 gateway is part of an HPE Aruba Networking Central group that has the settings shown in the exhibit. What would cause the gateway to drop traffic as part of its IDPS settings?

A. Its site-to-site VPN connections failing

B. Traffic matching a rule in the active ruleset

C. Its IDPS engine failing

D. Traffic showing anomalous behavior

Answer: B

Explanation:

In the exhibit, the HPE Aruba Networking Central settings for the 9x00 gateway show that traffic inspection is enabled, and the gateway is set to operate in IDS (Intrusion Detection System) mode with the fail strategy set to "Block". This configuration means that the gateway will drop traffic if it matches a rule in the active ruleset.

1. Active Ruleset: The ruleset version 9861 is active, and the gateway is configured to automatically update the ruleset daily.

2. Traffic Matching Rules: When traffic matches a rule in the active ruleset, it is flagged as suspicious or malicious.

3. Block Mode: Since the fail strategy is set to "Block", any traffic that matches a rule in the active ruleset will be dropped to prevent potential threats.

Reference: The documentation for HPE Aruba Networking Central and gateway IDS/IPS configuration provides detailed information on how traffic is inspected and the implications of different fail strategies, including blocking traffic that matches the active ruleset.

Question: 54

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: 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.

Reference: Aruba's AOS-CX and UBT configuration guides detail the steps for setting up reserved VLANs for tunneling traffic to gateways.

Question: 55

You are establishing a cluster of HPE Aruba Networking ClearPass servers. (Assume that they are running version 6.9.).

For which type of certificate it is recommended to install a CA-signed certificate on the Subscriber before it joins the cluster?

A. Database

B. HTTPS

C. RADIUS/EAP

D. RadSec

Answer: B

Explanation:

When establishing a cluster of HPE Aruba Networking ClearPass servers, it is recommended to install a CA-

signed certificate for HTTPS on the Subscriber before it joins the cluster. This ensures secure communication between the servers in the cluster and provides a trusted certificate for client connections.

1. HTTPS Security: A CA-signed certificate for HTTPS ensures that all web-based communication to and from the ClearPass server is encrypted and secure.
2. Cluster Communication: Secure communication between ClearPass nodes in the cluster is essential for synchronization and data integrity.
3. Client Trust: Clients accessing the ClearPass server will trust the CA-signed certificate, avoiding security warnings and ensuring smooth operations.

Reference: ClearPass documentation and best practices for clustering and certificate management recommend installing CA-signed certificates for secure HTTPS communication.

Question: 56

You are setting up an HPE Aruba Networking VIA solution for a company. You have already created a VPN pool with IP addresses for the remote clients. During tests, however, the clients do not receive IP addresses from that pool.

What is one setting to check?

A. That the pool uses valid, public IP addresses that are assigned to the company
B. Thatthe pool is associated with the role to which the VIA clients are being assigned
C. Thatthe pool uses an IP subnet that is different from any subnet configured on the VPNC
D. That the pool is referenced in the clients' VIA Connection Profile

Answer: B

Explanation:

If VIA clients are not receiving IP addresses from the configured VPN pool, one setting to check is whether

the pool is associated with the role to which the VIA clients are being assigned. The association between the IP pool and the role ensures that clients assigned to that role receive IP addresses from the correct pool.

1. Role Association: Each role can be associated with a specific IP pool, ensuring that clients assigned to the role receive addresses from the intended pool.
2. IP Allocation: Proper configuration of the IP pool and its association with the role is crucial for correct IP address allocation.
3. IA Configuration: Ensuring that all settings, including IP pool associations, are correctly configured, facilitates seamless client connectivity.

Reference: Aruba's VIA configuration guides provide detailed steps for setting up VPN pools and associating them with client roles to ensure correct IP address allocation.

Question: 57

What is a typical use case for using HPE Aruba Networking ClearPass Onboard to provision devices?

A. Enabling unmanaged devices to succeed at certificate-based 802.1X

B. Enabling managed Windows domain computers to succeed at certificate-based 802.1X

C. Enhancing security for loT devices that need to authenticate with MAC-Auth

D. Enforcing posture-based assessment on managed Windows domain computers

Answer: A

Explanation:

A typical use case for using HPE Aruba Networking ClearPass Onboard is to provision unmanaged devices to succeed at certificate-based 802.1X authentication. ClearPass Onboard allows users to securely configure their personal devices with the necessary certificates and network settings to authenticate on the network using 802.1X, which enhances security and simplifies the onboarding process for unmanaged devices.

1. Certificate-Based Authentication: ClearPass Onboard simplifies the process of issuing and installing certificates on unmanaged devices, ensuring they can authenticate securely using 802.1X.

2. User-Friendly Onboarding: The Onboard process is user-friendly, guiding users through the steps needed to configure their devices for network access.

3. Enhanced Security: By using certificates for authentication, the solution provides a higher level of security compared to traditional username/password methods.

Reference: ClearPass Onboard documentation highlights the use of the platform for provisioning certificates on unmanaged devices to facilitate secure network access via 802.1X.

Question: 58

A company is using HPE Aruba Networking Central SD-WAN Orchestrator to establish a hub-spoke VPN between branch gateways (BGWs) at 1444 site and

VPNCs at multiple data centers.

What is part of the configuration that admins need to complete?

A. At the global level, create default IPsec policies for the SD-WAN Orchestrator to use.

B. In BGWs' groups, select the VPNCs to which to connect in a DC preference list.

C. In VPNCs' groups, establish VPN pools to control which branches connect to which VPNCs.

D. In BGWs' and VPNCs' groups, create default IKE policies for the SD-WAN Orchestrator to use.

Answer: B

Explanation:

When using HPE Aruba Networking Central SD-WAN Orchestrator to establish a hub-spoke VPN between branch gateways (BGWs) and VPN concentrators (VPNCs) at multiple data centers, admins need to configure the BGWs' groups by selecting the VPNCs to which they should connect in a Data Center (DC) preference list. This configuration ensures that branch gateways are properly directed to the preferred VPN concentrators, optimizing the hub-spoke VPN topology.

1. DC Preference List: This list allows administrators to prioritize which data center VPNCs the BGWs should connect to, ensuring efficient routing and redundancy.

2. Hub-Spoke Configuration: Properly setting the DC preference list is essential for establishing the desired hub-spoke VPN architecture.

3. Optimized Connectivity: This setup helps in optimizing traffic flow and maintaining connectivity between branches and data centers.

Reference: SD-WAN Orchestrator configuration guides provide detailed steps for setting up hubspoke VPN topologies and configuring DC preference lists for BGWs.

Question: 59

A company has HPE Aruba Networking APs (AOS-10), which authenticate clients to HPE Aruba Networking ClearPass Policy Manager (CPPM). CPPM is set up

to receive a variety of information about clients' profile and posture. New information can mean that CPPM should change a client's enforcement profile.

What should you set up on the APs to help the solution function correctly?

A. In the security settings, configure dynamic denylisting.

B. In the RADIUS server settings for CPPM, enable Dynamic Authorization.

C. In the WLAN profiles, enable interim RADIUS accounting.

D. In the RADIUS server settings for CPPM, enable querying the authentication status.

Answer: B

Explanation:

To ensure that HPE Aruba Networking APs (AOS-10) properly interact with HPE Aruba Networking ClearPass Policy Manager (CPPM) and dynamically update a client's enforcement profile based on new profile and posture information, you should enable Dynamic Authorization in the RADIUS server settings for CPPM. This allows ClearPass to send Change of Authorization (CoA) requests to the APs, prompting them to reapply the appropriate enforcement profiles based on updated information.

1. Dynamic Authorization: Enabling this feature allows ClearPass to dynamically push changes to the

APs whenever there is new relevant information about a client's profile or posture.

2. Change of Authorization (CoA): This mechanism ensures that clients are assigned the correct enforcement profiles in real-time, based on the latest data.

3. Enhanced Policy Enforcement: This setup helps in maintaining accurate and up-to-date policy enforcement for clients on the network.

Reference: ClearPass and AOS-10 documentation on RADIUS server settings and dynamic authorization explain the process and benefits of enabling Dynamic Authorization for real-time policy updates.

Question: 60

A company wants HPE Aruba Networking ClearPass Policy Manager (CPPM) to respond to Syslog messages from its Check Point firewall. You have added the

firewall as an event source and set up an event service. However, test Syslog messages are not triggering the expected actions.

What is one CPPM setting that you should check?

A. ClearPass Device Insight integration is disabled.

B. The Check Point Extension is installed through ClearPass Guest.

C. The CoA delay value is set to 0 on the server.

D. Ingress Event Dictionaries for Check Point messages are enabled.

Answer: D

Explanation:

To ensure that HPE Aruba Networking ClearPass Policy Manager (CPPM) responds correctly to Syslog messages from a Check Point firewall, you need to check that the Ingress Event Dictionaries for Check Point messages are enabled. These dictionaries are necessary for CPPM to properly interpret and respond to the Syslog messages received from the firewall.

1. Event Dictionaries: Ingress Event Dictionaries allow CPPM to understand the specific format and content of Syslog messages from various sources, such as Check Point firewalls.

2. Message Interpretation: Without these dictionaries enabled, CPPM may not correctly interpret the Syslog messages, leading to a failure in triggering the expected actions.

3. Configuration Check: Ensuring that the dictionaries are enabled is crucial for the proper functioning of the event service and accurate response to security events.

Reference: ClearPass documentation on Syslog integration and event service setup provides information on configuring Ingress Event Dictionaries for different event sources.

Question: 61

An AOS-CX switch has been configured to implement UBT to a cluster of three HPE Aruba Networking gateways.

How does the switch determine to which gateways to tunnel UBT users' traffic?

A. The switch tunnels all users' traffic to the gateway configured as the primary gateway in the UBT zone, unless that gateway fails.

B. The switch tunnels each user's traffic to the particular gateway assigned as that user's active user designed gateway.

C. The switch load balances client traffic across the primary and standby gateway configured in the UBT zone.

D. The switch tunnels all users' traffic to the gateway assigned as the switch's active device designated gateway.

Answer: B

Explanation:

When an AOS-CX switch implements User-Based Tunneling (UBT) to a cluster of three HPE Aruba Networking gateways, the switch determines to which gateway to tunnel each user's traffic based on the particular gateway assigned as that user's active user designated gateway. This ensures that

traffic is efficiently distributed and managed according to the designated gateway for each user.

1. User Designated Gateway: Each user's traffic is tunneled to a specific gateway that has been designated for that

user, ensuring efficient handling of traffic.

2. Traffic Distribution: This method allows for balanced distribution of user traffic across multiple gateways, enhancing network performance and reliability.

3. Gateway Assignment: The switch uses the assigned gateway for each user to determine the tunneling path, ensuring that traffic is directed to the appropriate gateway.

Reference: Aruba's UBT and AOS-CX configuration guides detail the process of setting up and managing user-based tunneling, including the assignment of user designated gateways for traffic tunneling.

Question: 62

What correctly describes an HPE Aruba Networking AP's Device (TPM) certificate?

A. It is signed by an HPE Aruba Networking CA and is trusted by many HPE Aruba Networking solutions.

B. It works well as a captive portal certificate for guest SSIDs.

C. It is a self-signed certificate that should not be used in production.

D. It is installed on APs after they connect to and are provisioned by HPE Aruba Networking Central.

Answer: A

Explanation:

An HPE Aruba Networking AP's Device (TPM) certificate is signed by an HPE Aruba Networking Certificate Authority (CA) and is trusted by many HPE Aruba Networking solutions. This certificate is used for secure communications and device authentication within the Aruba network ecosystem.

1. CA-Signed Certificate: The Device (TPM) certificate is signed by a trusted Aruba CA, ensuring its authenticity and integrity.

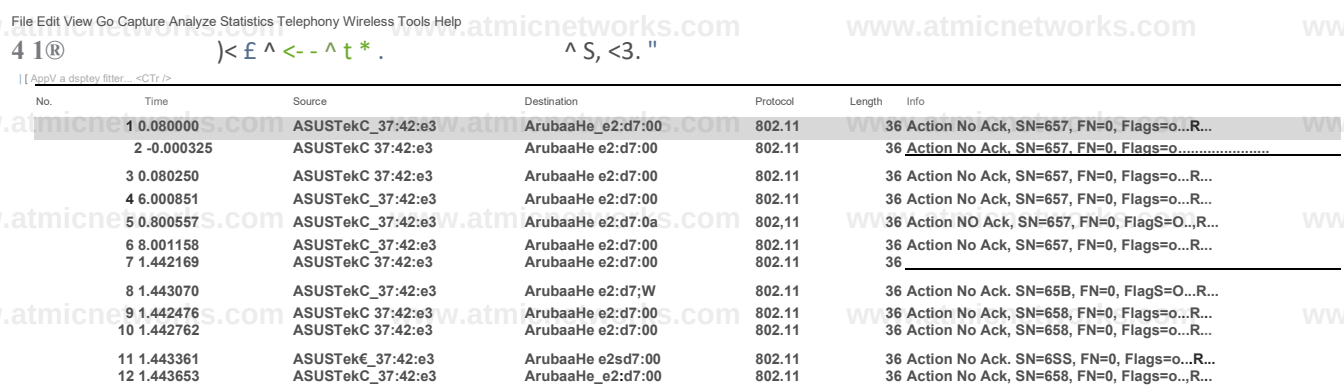
2. Trust Across Solutions: Because it is signed by an Aruba CA, it is recognized and trusted by various Aruba solutions, facilitating secure interactions and communications.

3. Security: Using a CA-signed certificate enhances the security of the network by preventing unauthorized access and ensuring that communications are secure.

Reference: Aruba's documentation on AP certificates and security protocols outlines the use and trust relationships of Device (TPM) certificates within the Aruba network infrastructure.

Question: 63

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:

To better interpret the packets shown in the Wireshark capture, you should choose to decode UDP port 5555 packets as ARUBA_ERM and set the Aruba ERM Type to 0. This configuration will allow Wireshark to properly decode and display the Aruba-specific encapsulated remote mirroring (ERM) packets, providing a clearer understanding of the traffic.

1. Decoding Protocols: Selecting the correct protocol decoding in Wireshark ensures that the captured packets are interpreted correctly, displaying the relevant information.
2. Aruba ERM: The packets in the capture are likely encapsulated remote mirroring (ERM) packets specific to Aruba, which require proper decoding settings in Wireshark.
3. Clear Interpretation: By setting the Aruba ERM Type to 0 and decoding the packets as ARUBA_ERM, you can view the encapsulated data accurately.

Reference: Wireshark documentation and Aruba network packet analysis guides provide instructions on setting protocol decoding options to accurately interpret specific types of network traffic, such as Aruba ERM packets.

Question: 64

A company wants to implement Virtual Network based Tunneling (VNBT) on a particular group of users and assign those users to an overlay network with VNI

3000.

Assume that an AOS-CX switch is already set up to:

. Implement 802.1X to HPE Aruba Networking ClearPass Policy Manager (CPPM)

. Participate in an EVPN VXLAN solution that includes VNI 3000

Which setting should you configure in the users' AOS-CX role to apply VNBT to them when they connect?

A. Gateway zone set to "3000" with no gateway role set

B. Gateway zone set to "vni-3000" with no gateway role set

C. Access VLAN set to the VLAN mapped to VNI 3000

D. Access VLAN ID set to "3000"

Answer: C

Explanation:

To apply Virtual Network based Tunneling (VNBT) to a particular group of users and assign them to an overlay network with VNI 3000, you should configure the users' AOS-CX role to set the Access VLAN to the VLAN mapped to VNI 3000. This ensures that when users connect, their traffic is tunneled through the specified VNI, integrating seamlessly with the EVPN VXLAN solution.

1. Access VLAN Configuration: Setting the Access VLAN to the VLAN mapped to VNI 3000 ensures that users' traffic is directed to the correct virtual network.
2. EVPN VXLAN Integration: This setup allows the AOS-CX switch to participate in the EVPN VXLAN solution, ensuring that user traffic is properly encapsulated and tunneled.
3. Role-Based Assignment: Configuring the role with the correct VLAN mapping ensures that users are dynamically assigned to the appropriate virtual network based on their role.

Reference: Aruba's documentation on AOS-CX configuration and VXLAN integration provides detailed steps for setting up VNBT and role-based VLAN assignments.

Question: 65

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?

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.

Reference: Aruba's ClearPass integration guides detail how CPDI and CPPM can work together to enhance security by leveraging device insights and dynamic policy enforcement.

Question: 66

What role can Internet Key Exchange (IKE)/IKEv2 play in an HPE Aruba Networking client-to-site VPN?

A. It provides an alternative to IPsec that is suitable for legacy clients.
B. It provides a more modern and secure alternative to IPsec.
C. It helps to negotiate the IPsec SA automatically and securely.
D. It helps remote clients download IPsec profiles for later use.

Answer: C

Explanation:

Internet Key Exchange (IKE)/IKEv2 plays a crucial role in an HPE Aruba Networking client-to-site VPN by helping to negotiate the IPsec Security Association (SA) automatically and securely. IKE/IKEv2 handles the authentication and key exchange processes, ensuring that both the client and the VPN gateway can establish a secure IPsec tunnel.

1. SA Negotiation: IKE/IKEv2 automates the negotiation of the Security Association, which defines the parameters for the secure IPsec tunnel.
2. Secure Authentication: It provides a secure method for authenticating the communicating parties and exchanging cryptographic keys.
3. Efficiency: Using IKE/IKEv2 simplifies the setup and maintenance of secure VPN connections, enhancing the overall security and reliability of the VPN.

Reference: Documentation on IPsec VPNs and IKE/IKEv2 protocols explains how these protocols facilitate secure and automated negotiation of IPsec tunnels, ensuring robust client-to-site VPN connections.

Question: 67

A company uses HPE Aruba Networking ClearPass Policy Manager (CPPM) as a TACACS+ server to authenticate managers on its AOS-CX switches. The company wants CPPM to control which commands managers are allowed to enter.

Which service must you add to the managers' TACACS+ enforcement profile?

A. Cpass:HTTP

B. Shell

C. ARAP

D. Aruba:Common

Answer: B

Explanation:

To control which commands managers are allowed to execute on AOS-CX switches using ClearPass Policy Manager (CPPM) as a TACACS+ server, you must configure the Shell service in the TACACS+ enforcement profile. The Shell service provides the ability to define granular access controls for commands. It supports policy-driven command authorization, which is essential in controlling administrative tasks based on roles.

Reference

Official HPE Aruba ClearPass documentation on TACACS+ integration and command authorization.

Industry best practices for AAA (Authentication, Authorization, and Accounting) configuration in network security architectures.

Question: 68

An AOS-CX switch has this admin user account configured on it:

netadmin in the operators group.

You have configured these commands on an AOS-CX switch:

tacacs-server host cp.example.com key plaintext &12xl,powmay7855

aaa authentication login ssh group tacacs local

aaa authentication allow-fail-through

A user accesses the switch with SSH and logs in as netadmin with the correct password. When the switch sends a TACACS+ request to the ClearPass server at cp.example.com, the server does not send a response. Authentication times out.

What happens?

A. The user is logged in and granted operator access.

B. The user is logged in and allowed to enter auditor commands only.

C. The user is logged in and granted administrators access.

D. The user is not allowed to log in.

Answer: A

Explanation:

Comprehensive Detailed Explanation

The configuration includes the command aaa authentication allow-fail-through, which specifies that if the TACACS+ server fails to respond (e.g., times out), the switch will proceed to the next authentication method in the sequence, which is local. In this scenario:

The switch first attempts to authenticate the user against the TACACS+ server.

When the TACACS+ server fails to respond, the switch falls back to local authentication.

The user netadmin is a local account configured on the switch and belongs to the operators group.

As a result, the user is successfully authenticated locally and is granted operator level access.

Reference

Aruba AOS-CX User Guide: Authentication fallback mechanisms.

TACACS+ fallback behavior for HPE Aruba switches.

Question: 69

A port-access role for AOS-CX switches has this policy applied to it:

plaintext

Copy code

port-access policy mypolicy

10 class ip zoneC action drop

20 class ip zoneA action drop

100 class ip zoneB

The classes have this configuration:

plaintext

Copy code

class ip zoneC

10 match tcp 10.2.0.0/16 eq https

class ip zoneA

10 match ip any 10.1.0.0/16

class ip zoneB

10 match ip any 10.0.0.0/8

The company wants to permit clients in this role to access 10.2.12.0/24 with HTTPS. What should you do?

A. Add this rule to zoneC: 5 matchany 10.2.12.0/24 eq https

B. Add this rule to zoneA: 5 ignore tcp any 10.2.12.0/24 eq https

C. Add this rule to zoneB: 5 match tcp any 10.2.12.0/24 eq https

D. Add this rule to zoneC: 5 ignore tcp any 10.2.12.0/24 eq https

Answer: A

Explanation:

Comprehensive Detailed Explanation

The requirement is to permit HTTPS traffic from clients to the 10.2.12.0/24 subnet.

ZoneC is configured to drop all HTTPS traffic to the 10.2.0.0/16 subnet. Therefore, the first match in the zoneC class (priority 10) will drop the desired traffic.

To override this behavior, you must add a higher-priority rule (lower rule number) to zoneC that explicitly matches 10.2.12.0/24 and permits the traffic.

Thus, adding the rule 5 match any 10.2.12.0/24 eq https to zoneC ensures the desired traffic is permitted while maintaining the drop behavior for the rest of 10.2.0.0/16.

Reference

AOS-CX Role-Based Access Control documentation.

Understanding class priority and policy rule ordering in AOS-CX.

Question: 70

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: A

Explanation:

Comprehensive Detailed Explanation

To prohibit users from uploading and downloading files from Dropbox using HPE Aruba Networking SSE (Secure Service Edge), you need to configure web access policies. This typically involves:

Adding a web category to the SSE configuration that includes Dropbox.

The SSE solution uses category-based filtering to block access to specific applications or services, such as Dropbox, based on their classification.

Other Options:

B . Installing the SSE root certificate is required for enabling SSL inspection, but this does not directly control access to Dropbox.

C and D. Deploying a connector is not necessary for this purpose as the enforcement is done via SSE policies, not by directly interfacing with Dropbox or remote users.

Reference

Aruba Networking SSE documentation on web filtering policies.

HPE Aruba SSE Application Control Best Practices Guide.

Question: 71

You are setting up user-based tunneling (UBT) between access layer AOS-CX switches and AOS-10 gateways. You have selected reserved (local) VLAN mode.

Tunneled devices include IoT devices, which should be assigned to:

Roles: iot on the switches and iot-wired on the gateways

VLAN: 64, for which the gateways route traffic.

IoT devices connect to the access layer switches' edge ports, and the access layer switches reach the gateways on their uplinks.

Where must you configure VLAN 64?

A. In the iot-wired role and on no physical interfaces

B. In the iot role and the iot-wired role and on no physical interfaces

C. In the iot-wired role and the access switch uplinks

D. In the iot role and the access switch uplinks

Answer: A

Explanation:

Comprehensive Detailed Explanation

In a user-based tunneling (UBT) setup with reserved VLAN mode, VLAN 64 is used for routing traffic at the gateways. Since the IoT traffic is tunneled to the AOS-10 gateway:

On the gateways:

VLAN 64 must be configured in the iot-wired role for routing purposes.

On the switches:

VLAN 64 does not need to be configured on the access switch physical uplinks because the IoT traffic is tunneled directly to the gateway and does not rely on VLAN configurations at the access layer switches.

Reserved VLAN mode:

Ensures that traffic is encapsulated within the UBT tunnel, and VLANs like 64 are only relevant at the gateway for routing and enforcement.

Therefore, the correct configuration is to define VLAN 64 in the iot-wired role on the AOS-10 gateways and not on any physical interfaces.

Reference

Aruba AOS-CX UBT configuration guide.

Aruba AOS-10 Gateway Role and VLAN Management documentation.

Question: 72

A company has a third-party security appliance deployed in its data center. The company wants to pass all traffic for certain clients through that device before forwarding that traffic toward its ultimate destination.

Which AOS-CX switch technology fulfills this use case?

A. Virtual Network Based Tunneling (VNBT)

B. MC-LAG

C. Network Analytics Engine (NAE)

D. Device profiles

Answer: A

Explanation:

Comprehensive Detailed Explanation

Virtual Network Based Tunneling (VNBT) is the appropriate technology for this use case because:

Traffic Steering: VNBT enables traffic from specific clients or devices to be tunneled through a predefined network path. This allows traffic to pass through intermediate devices such as third-party

security appliances.

Policy Enforcement: VNBT can be configured to route traffic based on roles, VLANs, or other policy definitions, ensuring that only specified traffic flows are redirected to the security appliance.

Scalability: This approach simplifies the redirection of traffic without requiring complex physical rewiring or changes to the underlying network topology.

Other Options:

MC-LAG: Primarily used for high-availability and redundancy in multi-chassis link aggregation scenarios, not for traffic redirection through appliances.

Network Analytics Engine (NAE): Used for monitoring and analytics, not traffic steering or forwarding.

Device Profiles: Helps automate switch port configurations for specific device types but does not handle traffic redirection.

Reference

AOS-CX Virtual Network Based Tunneling (VNBT) documentation.

Aruba Switch Architecture and Traffic Flow Control Best Practices Guide.

Question: 73

You manage AOS-10 APs with HPE Aruba Networking Central. A role is configured on these APs with the following rules:

Allow UDP on port 67 to any destination

Allow any to network 10.1.6.0/23

Deny any to network 10.1.0.0/16 + log

Deny any to network 10.0.0.0/8

Allow any to any destination

You add this new rule immediately before rule 2:

Deny SSH to network 10.1.4.0/23 + denylist

What happens when a client assigned to this role sends SSH traffic to 10.1.11.42?

A. The traffic is permitted.

B. The traffic is dropped and logged.

C. The traffic is dropped (without any logging or further action against the client).

D. The traffic is dropped, and the client is denylisted.

Answer: A

Explanation:

Comprehensive Detailed Explanation

Traffic Match Evaluation Order:

The rules are processed in sequential order, and the first rule that matches is applied.

The added rule only denies SSH traffic to 10.1.4.0/23. Since 10.1.11.42 is not within the 10.1.4.0/23 subnet, this rule does not apply.

Next Matching Rule:

Rule 2 permits traffic to the 10.1.6.0/23 network, but this does not include 10.1.11.42.

Rule 3 denies traffic to the broader 10.1.0.0/16 network and logs it. Since 10.1.11.42 falls under this range, this rule applies, and the traffic would be logged and dropped.

Logging and Denylist Actions:

The denylist action in the new rule only applies to SSH traffic to 10.1.4.0/23. Since the destination is outside that range, the denylist is not triggered.

Reference

Aruba AOS-10 Role and Firewall Rules Documentation.

HPE Aruba Central Configuration Best Practices Guide.

Question: 74

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:

Comprehensive Detailed Explanation

HPE Aruba Networking ClearPass Device Insight (CPDI) uses machine learning to assign endpoints to clusters and provide classification recommendations. For CPDI to automatically classify endpoints, specific thresholds of confidence and supporting classified devices must be met.

The generally required thresholds are:

Minimum Confidence Level: Typically, CPDI requires a recommendation confidence level of at least 95%.

Minimum Supporting Devices: CPDI needs a cluster to include at least 10 classified devices to ensure the recommendation is statistically meaningful.

Analysis of Each Option:

A . 96% confidence with 13 classified devices: Meets both thresholds (confidence > 95% and ≥ 10 devices). CPDI will automatically classify endpoints in this scenario.

B . 98% confidence with 5 classified devices: Confidence level is sufficient, but the cluster lacks the minimum required 10 classified devices. Automatic classification does not occur.

C . 93% confidence with 36 classified devices: The confidence level is below the required 95%. Automatic classification does not occur.

D . 100% confidence with 4 classified devices: Confidence is ideal, but there are insufficient supporting classified devices. Automatic classification does not occur.

Reference

HPE Aruba ClearPass Device Insight Deployment Guide.

Aruba ClearPass Machine Learning and Device Classification Thresholds.

Question: 75

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:

Comprehensive Detailed Explanation

A non-default device posture is applied in scenarios where specific checks on a device's compliance or security state (posture) are required to grant or deny access. The correct answer is:

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

This use case explicitly requires device posture assessment, which involves evaluating the device for attributes like antivirus software, patch levels, or other compliance criteria.

Non-default device posture rules are configured to assess these conditions and enforce the appropriate policy based on the device's state.

Other Options:

A . Applying threat inspection: Threat inspection rules operate independently of device posture and apply based on traffic content, not device compliance.

C . Redirecting compromised clients: This action is typically triggered based on a security event or threat detection, not directly related to device posture evaluation.

D . Integrating with ClearPass OnGuard: While OnGuard can contribute to posture assessment, it does not require a

non-default device posture in the SSE rule directly.

Reference

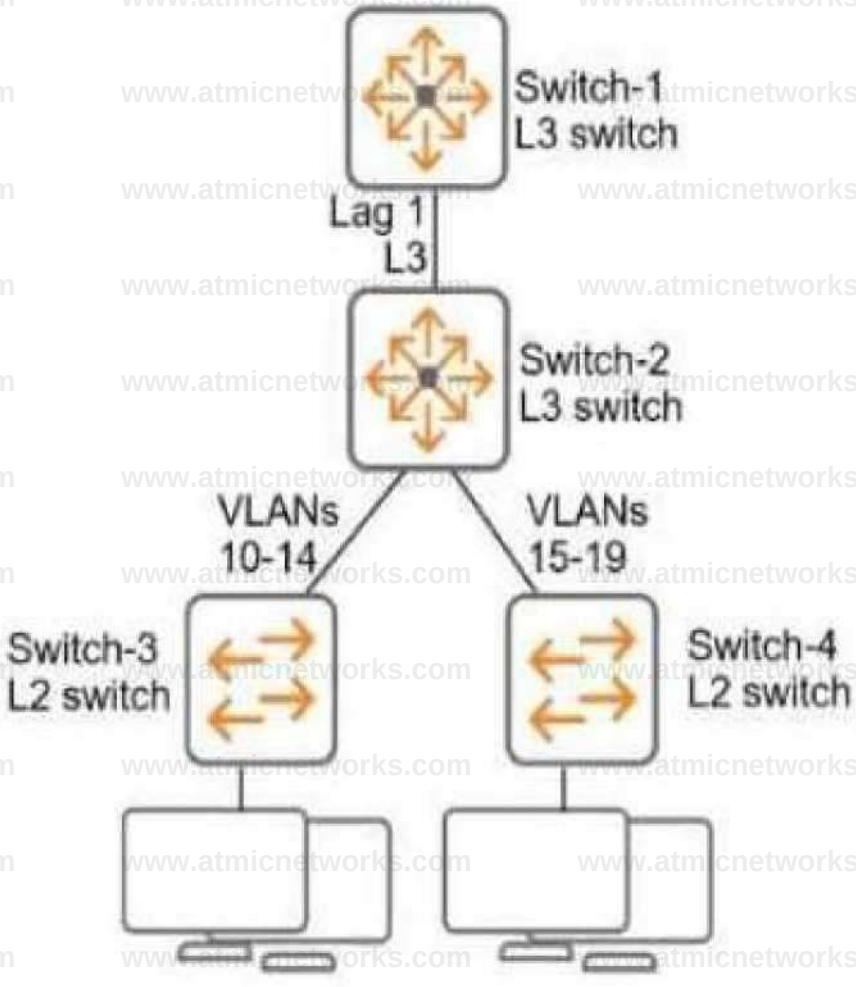
HPE Aruba SSE Posture-Based Access Control documentation.

Aruba ClearPass and SSE Integration Deployment Guide.

Question: 76

Refer to the exhibit.

Refer to Exhibit:



All of the switches in the exhibit are AOS-CX switches.

What is the preferred configuration on Switch-2 for preventing rogue OSPF routers in this network?

A. Configure OSPF authentication on VLANs 10-19 in password mode.

B. Configure OSPF authentication on Lag 1 in MD5 mode.

C. Disable OSPF entirely on VLANs 10-19.

D. Configure passive-interface as the OSPF default and disable OSPF passive on Lag 1.

Answer: B

Explanation:

Why MD5 Authentication on Lag 1 is Preferred:

Lag 1 is the primary link between Switch-2 and Switch-1, both of which are Layer 3 switches running OSPF.

By enabling MD5 authentication, OSPF routers exchange authenticated packets, preventing unauthorized or rogue OSPF routers from forming adjacencies or injecting routes.

MD5 is a secure authentication method and ensures the integrity and authenticity of OSPF communications.

Other Options Analysis:

A . Configure OSPF authentication on VLANs 10-19 in password mode: While configuring authentication on VLAN interfaces could secure VLAN-specific OSPF traffic, it is less effective because the main threat of rogue OSPF comes from unauthorized L3 devices connected via the backbone (Lag 1).

C . Disable OSPF entirely on VLANs 10-19: Disabling OSPF on these VLANs is not a preferred solution because OSPF is needed to route traffic in this design.

D . Configure passive-interface as the OSPF default and disable OSPF passive on Lag 1: While passive interfaces prevent OSPF from forming adjacencies, it does not directly prevent rogue routers. Passive mode only limits OSPF advertisements on specific interfaces.

Question: 77

Which issue can an HPE Aruba Networking Secure Web Gateway (SWG) solution help customers address?

A. The organization needs a faster way to quarantine clients that have generated threats, as detected by third-party firewalls.

B. Hybrid workers are exposing their computers to risky internet sites and infection by malware when they work from home.

C. Remote workers need access to private data center applications without exposing those applications to unauthorized users.

D. The organization currently has no way to prevent users from exfiltrating sensitive data from SaaS applications.

Answer: B

Explanation:

An HPE Aruba Networking Secure Web Gateway (SWG) is designed to provide secure internet access by monitoring and controlling web traffic. It primarily focuses on protecting users from malicious content and ensuring compliance with corporate security policies, particularly for hybrid and remote workers.

Explanation of Each Option

A . The organization needs a faster way to quarantine clients that have generated threats, as detected by third-party firewalls.

Incorrect:

Quarantining clients based on detected threats is typically managed by endpoint detection and response (EDR) solutions or next-generation firewalls (NGFWs).

While an SWG can monitor and block risky web activity, it does not manage threat quarantine actions directly.

B . Hybrid workers are exposing their computers to risky internet sites and infection by malware when they work from home.

Correct:

SWGs monitor and control web traffic to block malicious websites and prevent exposure to malware.

They enforce web usage policies even when users work remotely, protecting against phishing, drive- by downloads, and other web-based threats.

With the proliferation of hybrid work environments, an SWG ensures that users are protected from risky sites regardless of their location.

C . Remote workers need access to private data center applications without exposing those applications to unauthorized users.

Incorrect:

This use case falls under secure access service edge (SASE) solutions with Zero Trust Network Access (ZTNA), not an SWG.

ZTNA focuses on granting secure, conditional access to applications, while SWGs focus on internet traffic security.

D . The organization currently has no way to prevent users from exfiltrating sensitive data from SaaS applications.

Incorrect:

Data loss prevention (DLP) tools or cloud access security brokers (CASBs) are designed for monitoring and preventing data exfiltration from SaaS applications.

While SWGs can block access to specific websites or categories, they do not offer advanced DLP capabilities for SaaS environments.

Reference

Aruba Secure Web Gateway Documentation.

HPE Aruba SASE Solutions Guide.

Best Practices for Hybrid Workforce Security with Aruba SWG.

Question: 78

A company has several use cases for using its AOS-CX switches' HPE Aruba Networking Network Analytics Engine (NAE).

What is one guideline to keep in mind as you plan?

A. Each switch model has a maximum number of supported monitors, and one agent might have multiple monitors.

B. You can install multiple scripts on a switch, but you can deploy only one agent per script.

C. The switch will permit you to deploy as many NAE agents as you want, but they might degrade the switch functionality.

D. When you use custom scripts, you can create as many agents from each script as you want.

Answer: A

Explanation:

The Network Analytics Engine (NAE) in AOS-CX switches provides intelligent monitoring, troubleshooting, and performance analysis through predefined or custom scripts. Here's an analysis of the guidelines for NAE:

A . Each switch model has a maximum number of supported monitors, and one agent might have multiple monitors.

Correct:

Each AOS-CX switch model has hardware and software limitations, including the number of agents and monitors it supports.

Monitors are data collection points for tracking specific metrics like interface statistics, CPU usage, or custom-defined parameters.

Agents are scripts that use monitors to evaluate data, trigger actions, or generate alerts.

Since one agent can have multiple monitors, the total number of monitors might impact the scalability of agents.

B . You can install multiple scripts on a switch, but you can deploy only one agent per script.

Incorrect:

Multiple agents can be deployed from the same script if they monitor different parameters or have different configurations.

The limitation is usually related to the total number of agents and monitors supported by the switch model, not the script itself.

C . The switch will permit you to deploy as many NAE agents as you want, but they might degrade the switch functionality.

Incorrect:

AOS-CX enforces hardware and software limits on the number of agents and monitors. These limits are designed to prevent degradation of switch performance.

You cannot deploy an unlimited number of agents, as the system enforces these restrictions.

D . When you use custom scripts, you can create as many agents from each script as you want.

Incorrect:

While you can use custom scripts to create agents, the total number of agents is subject to the switch's maximum

supported limits.

The scalability of agents is still bound by hardware and software constraints, even with custom scripts.

Reference

HPE Aruba AOS-CX Network Analytics Engine Configuration Guide.

Aruba AOS-CX Switch Series Technical Specifications.

Best Practices for NAE Deployment in AOS-CX Networks.

Question: 79

A company has been running Gateway IDS/IPS on its gateways in IDS mode for several weeks. The company wants to transition to IPS mode.

What is one step you should recommend?

A. Disable traffic inspection and reboot before re-enabling traffic inspection with the new mode.

B. Change the mode on one gateway at a time to establish a smoother transition period.

C. Consider applying a stricter IPS policy to minimize issues during the transition period.

D. Check for legitimate traffic that has been flagged as a threat and allow list the associated rules.

Answer: D

Explanation:

When transitioning from Intrusion Detection System (IDS) mode to Intrusion Prevention System (IPS) mode, it's critical to review and refine configurations to ensure legitimate traffic is not blocked.
Here's the reasoning behind each option:

A . Disable traffic inspection and reboot before re-enabling traffic inspection with the new mode.

Incorrect:

Transitioning to IPS mode does not require a full reboot or disabling traffic inspection.

This step is unnecessary and could lead to downtime that impacts network operations.

B . Change the mode on one gateway at a time to establish a smoother transition period.

Incorrect:

While a phased approach might help in some large deployments, it does not directly address the potential for legitimate traffic to be blocked by IPS mode.

IPS operates in real-time, so misconfigured rules or policies need to be addressed before enabling IPS on any gateway.

C . Consider applying a stricter IPS policy to minimize issues during the transition period.

Incorrect:

A stricter IPS policy increases the likelihood of false positives, which could disrupt legitimate business-critical traffic.

During the transition, the focus should be on minimizing disruptions by fine-tuning policies, not making them stricter.

D . Check for legitimate traffic that has been flagged as a threat and allow list the associated rules.

Correct:

In IDS mode, the system only detects and logs suspicious traffic but does not block it. Reviewing these logs for false positives allows the organization to fine-tune policies and allow list legitimate

traffic before transitioning to IPS mode.

By doing this, the company ensures that IPS mode will block actual threats while permitting legitimate traffic.

This is a proactive step to prevent unnecessary disruptions to normal operations when IPS mode is enabled.

Reference

HPE Aruba Gateway IDS/IPS Configuration Guide.

Best Practices for Transitioning from IDS to IPS Modes in Aruba Networks.

Aruba Network Threat Management Documentation.

Question: 80

A ClearPass Policy Manager (CPPM) service includes these settings:

Role Mapping Policy:

Evaluate: Select first

Rule 1 conditions:

Authorization:AD:Groups EQUALS Managers

Authentication:TEAP-Method-1-Status EQUALS Success

Rule 1 role: manager

Rule 2 conditions:

Authentication:TEAP-Method-1-Status EQUALS Success

Rule 2 role: domain-comp

Default role: [Other]

Enforcement Policy:

Evaluate: Select first

Rule 1 conditions:

Tips Role EQUALS manager AND Tips Role EQUALS domain-comp

Rule 1 profile list: domain-manager

Rule 2 conditions:

Tips Role EQUALS manager

Rule 2 profile list: manager-only

Rule 3 conditions:

Tips Role EQUALS domain-comp

Rule 3 profile list: domain-only

Default profile: [Deny access]

A client is authenticated by the service. CPPM collects attributes indicating that the user is in the Contractors group, and the client passed both TEAP methods.

Which enforcement policy will be applied?

A. [Deny Access Profile]

B. manager-only

C. domain-manager

D. domain-only

Answer: A

Explanation:

1. Understanding the Role Mapping Evaluation:

Role mapping is set to "Evaluate: Select first," meaning the first rule that matches the client attributes will determine the role(s) assigned.

Contractors group: Since the client is in the Contractors group (not Managers), Rule 1 in the Role Mapping Policy does not match.

TEAP-Method-1-Status EQUALS Success: This condition matches Rule 2, so the client is assigned the domain-comp role.

No other rules match, so the default role [Other] is not applied.

2. Resulting Role from Role Mapping Policy:

The client is assigned the domain-comp role.

3. Enforcement Policy Evaluation:

Enforcement policy is also set to "Evaluate: Select first," so the first matching rule determines the enforcement profile.

Rule 1 (Tips Role = manager AND domain-comp):

The client only has the domain-comp role, not manager, so this rule does not match.

Rule 2 (Tips Role = manager):

The client does not have the manager role, so this rule does not match.

Rule 3 (Tips Role = domain-comp):

This rule matches the client's role, but it is not evaluated because the enforcement policy already skipped to the default action after failing the first two rules.

4. Default Enforcement Profile:

Since no rule explicitly matches and the policy evaluation stops at the default, the default profile [Deny Access Profile] is applied.

Final Outcome:

The client is denied access because none of the matching rules satisfy the conditions.

Reference

Aruba ClearPass Policy Manager Role Mapping and Enforcement Policies Guide.

Role and Policy Evaluation Logic for ClearPass Authentication Services.

Question: 81

A company has HPE Aruba Networking APs managed by HPE Aruba Networking Central. You have set up a WLAN to enforce WPA3 with 802.1X authentication.

What happens if the client fails authentication?

A. The AP assigns the client to the WLAN's default role.

B. The AP drops the client because authentication aborts.

C. The AP assigns the client to the WLAN's critical role.

D. The AP assigns the client to the WLAN's initial role.

Answer: B

Explanation:

When WPA3 with 802.1X authentication is enforced on an HPE Aruba Networking WLAN, the authentication process strictly adheres to security standards. Here's how the process works:

1. 802.1X Authentication Workflow in WPA3

The client must provide valid credentials (such as certificates or username/password) to authenticate with the RADIUS server via 802.1X.

If the client fails authentication (e.g., due to invalid credentials or lack of proper configuration), the 802.1X handshake fails, and the AP terminates the connection.

2. Role Assignment in WLANs

Default Role: The role assigned to authenticated clients after a successful 802.1X authentication. It is not applied to unauthenticated clients.

Critical Role: This is a fallback role applied when there are issues communicating with the RADIUS server, not when authentication fails.

Initial Role: A temporary role assigned to clients before authentication completes. However, this role is removed once the authentication process determines failure.

3. Behavior Upon Authentication Failure

In the case of an authentication failure, the client does not get assigned to any role (default, critical, or initial) because it does not meet the conditions for network access.

The client is dropped immediately, and no further communication is allowed until reauthentication is attempted.

Explanation of Each Option

A . The AP assigns the client to the WLAN's default role:

Incorrect: The default role applies only after successful authentication, not in case of authentication failure.

B . The AP drops the client because authentication aborts:

Correct: If the client fails authentication, the AP terminates the connection without assigning any roles.

C . The AP assigns the client to the WLAN's critical role:

Incorrect: The critical role is used when the AP cannot reach the RADIUS server, not when authentication fails.

D . The AP assigns the client to the WLAN's initial role:

Incorrect: The initial role is applied during the authentication process, but it is not retained after a failed authentication.

Reference

Aruba Central WLAN Configuration Guide.

WPA3 and 802.1X Authentication Best Practices in Aruba Networks.

Aruba AP Role Assignment Workflow Documentation.

Question: 82

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

What is one aspect of the integration that you should explain?

A. CPPM no longer supports any Device Profiler features and relies on CPDI for this profile information.

B. CPDI must be configured as an audit server on CPPM for the integration to be successful.

C. CPDI must have security analysis disabled on it for the integration to be successful.

D. CPPM can submit profile information to CPDI, but if CPDI derives a different classification, CPDI takes precedence.

Answer: D

Explanation:

When integrating ClearPass Policy Manager (CPPM) with ClearPass Device Insight (CPDI), it is important to understand how device profiling and classification work between the two solutions:

1. CPPM and CPDI Integration Overview

CPPM is primarily used for access control and policy enforcement, while CPDI specializes in device profiling and classification through advanced analytics and machine learning.

Integration allows CPPM to leverage CPDI's enhanced profiling capabilities for more accurate device identification and policy enforcement.

2. Detailed Analysis of Each Option

A . CPPM no longer supports any Device Profiler features and relies on CPDI for this profile information:

Incorrect: CPPM still supports its own basic device profiling features and can operate independently. However, when integrated with CPDI, CPPM can use CPDI's advanced profiling capabilities as a supplement.

B . CPDI must be configured as an audit server on CPPM for the integration to be successful:

Incorrect: CPDI is not configured as an audit server on CPPM. Integration is achieved via API integration and communication

between the two solutions, not through audit server settings.

C . CPDI must have security analysis disabled on it for the integration to be successful:

Incorrect: Security analysis does not need to be disabled for integration. In fact, CPDI's security analysis enhances the classification process by identifying anomalous behaviors.

D . CPPM can submit profile information to CPDI, but if CPDI derives a different classification, CPDI takes precedence:

Correct:

CPPM and CPDI exchange profile data, but CPDI has more advanced device classification capabilities due to its machine learning-based engine.

When CPDI derives a different classification than CPPM, CPDI's classification is considered more accurate and takes precedence.

This ensures that policies are based on the most reliable device classification.

Reference

Aruba ClearPass Policy Manager and Device Insight Integration Guide.

ClearPass Device Profiling and Classification Documentation.

Best Practices for CPPM and CPDI Integration in Network Security.

Question: 83

Refer to Exhibit:

An HPE Aruba Networking 9x00 gateway is part of an HPE Aruba Networking Central group that has the settings shown in the exhibit. What would cause the gateway to drop traffic as part of its IDPS

settings?

A. Its site-to-site VPN connections failing

B. Traffic matching a rule in the active ruleset

C. Its IDPS engine failing

D. Traffic showing anomalous behavior

Answer: B

Explanation:

1. IDPS Mode Configuration Overview

The exhibit shows the HPE Aruba Networking Central settings for the Gateway IDS/IPS configuration:

Mode: Configured for Intrusion Prevention System (IPS), meaning that the gateway actively blocks traffic identified as threats.

Fail Strategy: Configured to Block, meaning that if the gateway cannot determine the traffic's nature due to a system issue, it will block the traffic.

Ruleset: The gateway uses a predefined set of intrusion detection/prevention rules (ruleset version 9861), which is updated automatically every day.

2. Traffic Evaluation in IPS Mode

In IPS mode, the gateway analyzes traffic against the active ruleset:

If traffic matches a rule in the ruleset and is deemed malicious, the gateway will drop the traffic as part of its prevention mechanism.

The ruleset defines specific conditions (e.g., signatures of known attacks, protocol anomalies) under which traffic should be blocked.

3. Explanation of Each Option

A . Its site-to-site VPN connections failing:

Incorrect:

Site-to-site VPN connection issues do not directly trigger traffic drops under IDPS settings.

IDPS is focused on detecting and preventing malicious activity, not general connectivity issues.

B . Traffic matching a rule in the active ruleset:

Correct:

In IPS mode, the gateway drops traffic that matches any predefined rules in the active ruleset.

For example, if traffic matches the signature of a known exploit or attack, it is immediately blocked.

C . Its IDPS engine failing:

Incorrect:

The fail strategy determines how the gateway behaves in the event of an IDPS engine failure.

In this case, the fail strategy is set to Block, but this applies only if the engine itself fails, not as a proactive traffic drop mechanism.

D . Traffic showing anomalous behavior:

Incorrect:

While anomalous behavior may be logged or flagged, it does not necessarily lead to traffic drops unless it matches a specific rule in the active ruleset.

Anomaly detection alone is not sufficient for IPS action without explicit rule matches.

Final Outcome:

Traffic is dropped only when it matches a rule in the active ruleset, ensuring targeted prevention of malicious activity.

Reference

Aruba Gateway IDS/IPS Configuration Guide.

Aruba Central Ruleset Management Documentation.

Best Practices for Configuring Fail Strategies in IPS Mode.

Question: 84

You are establishing a cluster of HPE Aruba Networking ClearPass servers. (Assume that they are running version 6.9.).

For which type of certificate is it recommended to install a CA-signed certificate on the Subscriber before it joins the cluster?

A. HTTPS

B. Database

C. RADIUS/EAP

D. RadSec

Answer: A

Explanation:

When setting up a ClearPass cluster, it is critical to ensure secure communication between the cluster nodes and the client devices. For this purpose, certain certificates must be properly configured.

1. Why HTTPS Requires a CA-Signed Certificate?

HTTPS communication is used for inter-cluster communication and for the web-based user interface that administrators use to manage the ClearPass cluster.

Before joining the cluster, it is strongly recommended to install a CA-signed HTTPS certificate on the Subscriber to ensure secure communication and prevent warnings/errors due to untrusted certificates.

Without a CA-signed certificate, the Subscriber might use a self-signed certificate, leading to security risks and lack of trust validation.

2. Analysis of Other Certificate Types

B . Database:

Incorrect: Database communications within ClearPass clusters are secured using internal certificates or keys. These are not user-facing and do not require a CA-signed certificate before joining the cluster.

C . RADIUS/EAP:

Incorrect: RADIUS/EAP certificates are important for client authentication, but they are not required on the Subscriber prior to cluster joining. These can be configured after the Subscriber is part of the cluster.

D . RadSec:

Incorrect: RadSec is an optional feature for secure RADIUS communication over TLS, and its certificate configuration is typically performed post-cluster setup.

Final Recommendation

To ensure secure cluster operations and seamless web-based management, a CA-signed HTTPS certificate should be installed on the Subscriber before it joins the ClearPass cluster.

Reference

ClearPass Deployment Guide for Version 6.9.

Best Practices for Certificate Management in ClearPass Clusters.

HPE Aruba ClearPass Cluster Configuration Guide.

Question: 85

A company has HPE Aruba Networking gateways that implement gateway IDS/IPS. Admins sometimes check the Security Dashboard, but they want a faster way to discover if a gateway starts detecting threats in traffic.

What should they do?

A. Set up Webhooks that are attached to the HPE Aruba Networking Central Threat Dashboard.

B. Use Syslog to integrate the gateways with HPE Aruba Networking ClearPass Policy Manager (CPPM) event processing.

C. Set up email notifications using HPE Aruba Networking Central's global alert settings.

D. Integrate HPE Aruba Networking ClearPass Device Insight (CPDI) with Central and schedule hourly reports.

Answer: C

Explanation:

1. The Need for Faster Threat Notifications

Admins need immediate alerts when threats are detected by the gateway's IDS/IPS functionality. Regularly checking the Security Dashboard is inefficient, so an automated notification system is essential for faster response times.

2. Explanation of Each Option

A . Set up Webhooks that are attached to the HPE Aruba Networking Central Threat Dashboard:

Incorrect:

Webhooks are useful for integrating alerts with third-party tools or custom workflows. However, setting up email notifications through global alert settings is faster and simpler for this purpose.

B . Use Syslog to integrate the gateways with HPE Aruba Networking ClearPass Policy Manager (CPPM) event processing:

Incorrect:

Syslog integration with CPPM is typically used for logging and correlating events, not for real-time notifications about threats.

CPPM is better suited for policy enforcement, not instant threat alerts.

C . Set up email notifications using HPE Aruba Networking Central's global alert settings:

Correct:

HPE Aruba Networking Central has global alert settings that allow admins to configure email notifications for specific events, such as threat detection.

This is the simplest and most effective way to ensure admins receive immediate notifications when threats are detected by the gateways.

D . Integrate HPE Aruba Networking ClearPass Device Insight (CPDI) with Central and schedule hourly reports:

Incorrect:

While CPDI integration provides enhanced device profiling, it is not directly tied to gateway IDS/IPS threat detection.

Hourly reports are not real-time notifications and would not meet the requirement for faster threat alerts.

Final Recommendation

Setting up email notifications through HPE Aruba Networking Central's global alert settings provides the most direct and efficient solution for immediate threat detection alerts.

Reference

HPE Aruba Networking Central Alert Management Documentation.

Aruba IDS/IPS and Security Dashboard Configuration Guide.

Email Notification Setup for Aruba Central Threat Alerts.

Question: 86

A company has Aruba APs that are controlled by Central and that implement WIDS. When you check WIDS events, you see a "detect valid SSID misuse" event. What can you interpret from this event, and what steps should you take?

A. Clients are failing to authenticate to corporate SSIDs. You should first check for misconfigured authentication settings and then investigate a possible threat.

B. Admins have likely misconfigured SSID security settings on some of the company's APs. You should have them check those settings.

C. Hackers are likely trying to pose as authorized APs. You should use the detecting radio information and immediately track down the device that triggered the event.

D. This event might be a threat but is almost always a false positive. You should wait to see the event over several days before following up on it.

Answer: C

Explanation:

The "Detect Valid SSID Misuse" event in Aruba's Wireless Intrusion Detection System (WIDS) indicates that a valid SSID, associated with your network, is being broadcast from an unauthorized source. This scenario often signals a potential rogue access point attempting to deceive clients into connecting to it (e.g., for credential harvesting or man-in-the-middle attacks).

1. Explanation of Each Option

A . Clients are failing to authenticate to corporate SSIDs. You should first check for misconfigured authentication settings and then investigate a possible threat:

Incorrect:

This event is not related to authentication failures by legitimate clients.

Misconfigured authentication settings would lead to events like "authentication failures" or "radius issues," not "valid SSID misuse."

B . Admins have likely misconfigured SSID security settings on some of the company's APs. You should have them check those settings:

Incorrect:

This event refers to an external device broadcasting your SSID, not misconfiguration on the company's authorized APs.

WIDS differentiates between valid corporate APs and rogue APs.

C . Hackers are likely trying to pose as authorized APs. You should use the detecting radio information and immediately track down the device that triggered the event:

Correct:

This is the most likely cause of the "detect valid SSID misuse" event. A rogue AP broadcasting a corporate SSID could lure clients into connecting to it, exposing sensitive credentials or traffic.

Immediate action includes:

Using the radio information from the event logs to identify the rogue AP's location.

Physically locating and removing the rogue device.

Strengthening WIPS/WIDS policies to prevent further misuse.

D . This event might be a threat but is almost always a false positive. You should wait to see the event over several days before following up on it:

Incorrect:

While false positives are possible, "valid SSID misuse" is a critical security event that should not be ignored.

Delaying action increases the risk of successful attacks against your network.

2. Recommended Steps to Address the Event

Review Event Logs:

Gather details about the rogue AP, such as SSID, MAC address, channel, and signal strength.

Locate the Rogue Device:

Use the detecting AP's radio information and signal strength to triangulate the rogue AP's physical location.

Respond to the Threat:

Remove or disable the rogue device.

Notify the security team for further investigation.

Prevent Future Misuse:

Strengthen security policies, such as enabling client whitelists or enhancing WIPS protection.

Reference

Aruba WIDS/WIPS Configuration and Best Practices Guide.

Aruba Central Security Event Analysis Documentation.

Wireless Threat Management Using Aruba Networks.

Question: 87

A company is using HPE Aruba Networking ClearPass Device Insight (CPDI) (the standalone application). In the CPDI security settings, Security Analysis is On, the Data Source is ClearPass Device

Insight, and Enable Posture Assessment is On. You see that a device has a Risk Score of 90.

What can you know from this information?

A. The posture is unknown, and CPDI has detected exactly four vulnerabilities on the device.

B. The posture is healthy, but CPDI has detected multiple vulnerabilities on the device.

C. The posture is unhealthy, and CPDI has also detected at least one vulnerability on the device.

D. The posture is unhealthy, but CPDI has not detected any vulnerabilities on the device.

Answer: C

Explanation:

1. Understanding CPDI Risk Score and Posture Analysis

The Risk Score in ClearPass Device Insight (CPDI) is a numerical value representing the overall risk level associated with a device. It considers factors such as:

Posture Assessment: The device's compliance with health policies (e.g., OS updates, antivirus status).

Security Analysis: Vulnerabilities detected on the device, such as known exploits or weak configurations.

A Risk Score of 90 indicates a high-risk device, suggesting that the posture is unhealthy and vulnerabilities have been

detected.

2. Analysis of Each Option

A . The posture is unknown, and CPDI has detected exactly four vulnerabilities on the device:

Incorrect:

The posture cannot be "unknown" because posture assessment is enabled in the settings.

CPDI does not explicitly indicate the exact number of vulnerabilities directly through the Risk Score.

B . The posture is healthy, but CPDI has detected multiple vulnerabilities on the device:

Incorrect:

A Risk Score of 90 is too high for a "healthy" posture. A healthy posture would typically result in a lower Risk Score.

C . The posture is unhealthy, and CPDI has also detected at least one vulnerability on the device:

Correct:

A high Risk Score of 90 indicates an unhealthy posture.

The presence of vulnerabilities (based on Security Analysis being enabled) further justifies the high Risk Score.

This combination of unhealthy posture and detected vulnerabilities aligns with the Risk Score and configuration provided.

D . The posture is unhealthy, but CPDI has not detected any vulnerabilities on the device:

Incorrect:

If no vulnerabilities were detected, the Risk Score would not be as high as 90, even if the posture were unhealthy.

Final Interpretation

From the configuration and Risk Score provided, the device's posture is unhealthy, and at least one vulnerability has been detected by CPDI.

Reference

HPE Aruba ClearPass Device Insight Deployment Guide.

CPDI Risk Score Analysis and Security Settings Documentation.

Best Practices for Posture Assessment in Aruba Networks.

Question: 88

Which statement describes Zero Trust Security?

A. Companies must apply the same access controls to all users, regardless of identity.

B. Companies that support remote workers cannot achieve zero trust security and must determine if the benefits outweigh the cost.

C. Companies should focus on protecting their resources rather than on protecting the boundaries of their internal network.

D. Companies can achieve zero trust security by strengthening their perimeter security to detect a wider range of threats.

Answer: C

Explanation:

What is Zero Trust Security?

Zero Trust Security is a security model that operates on the principle of "never trust, always verify."

It focuses on securing resources (data, applications, systems) and continuously verifying the identity and trust level of users and devices, regardless of whether they are inside or outside the network.

The primary aim is to reduce reliance on perimeter defenses and implement granular access controls to protect individual resources.

Analysis of Each Option

A . Companies must apply the same access controls to all users, regardless of identity:

Incorrect:

Zero Trust enforces dynamic and identity-based access controls, not the same static controls for everyone.

Users and devices are granted access based on their specific context, role, and trust level.

B . Companies that support remote workers cannot achieve zero trust security and must determine if the benefits outweigh the cost:

Incorrect:

Zero Trust is particularly effective for securing remote work environments by verifying and authenticating remote users and devices before granting access to resources.

The model is adaptable to hybrid and remote work scenarios, making this statement false.

C . Companies should focus on protecting their resources rather than on protecting the boundaries of their internal network:

Correct:

Zero Trust shifts the focus from perimeter security (traditional network boundaries) to protecting specific resources.
This includes implementing measures such as:

Micro-segmentation.

Continuous monitoring of user and device trust levels.

Dynamic access control policies.

The emphasis is on securing sensitive assets rather than assuming an internal network is inherently safe.

D . Companies can achieve zero trust security by strengthening their perimeter security to detect a wider range of threats:

Incorrect:

Zero Trust challenges the traditional reliance on perimeter defenses (firewalls, VPNs) as the sole security mechanism.

Strengthening perimeter security is not sufficient for Zero Trust, as this model assumes threats can already exist inside the network.

Final Explanation

Zero Trust Security emphasizes protecting resources at the granular level rather than relying on the traditional security

perimeter, which makes C the most accurate description.

Reference

NIST Zero Trust Architecture Guide.

Zero Trust Principles and Implementation in Modern Networks by HPE Aruba.

"Never Trust, Always Verify" Framework Overview from Cybersecurity Best Practices.

Question: 89

A company has AOS-CX switches. The company wants to make it simpler and faster for admins to detect denial of service (DoS) attacks, such as ping or ARP floods, launched against the switches.

What can you do to support this use case?

A. Deploy an NAE agent on the switches to monitor control plane policing (CoPP).

B. Configure the switches to implement RADIUS accounting to HPE Aruba Networking ClearPass and enable HPE Aruba Networking ClearPass Insight.

C. Implement ARP inspection on all VLANs that support end-user devices.

D. Enabling debugging of security functions on the switches.

Answer: A

Explanation:

Why Monitoring Control Plane Policing (CoPP) with an NAE Agent Is Effective for Detecting DoS Attacks

Control Plane Policing (CoPP): AOS-CX switches use CoPP to protect the CPU from excessive traffic caused by DoS attacks (e.g., ARP floods, ICMP floods). CoPP enforces rate limits and drops malicious traffic at the control plane level.

NAE (Network Analytics Engine) Agent:

The NAE on AOS-CX switches can monitor CoPP counters in real time and trigger alerts if thresholds for certain traffic types (e.g., ICMP, ARP) are exceeded.

Admins can use NAE to automate detection and respond faster to DoS attacks.

Analysis of Each Option

A . Deploy an NAE agent on the switches to monitor control plane policing (CoPP):

Correct:

NAE agents provide real-time visibility into CoPP behavior, helping detect DoS attacks more quickly.

By analyzing CoPP statistics, the NAE can pinpoint abnormal traffic patterns and alert admins.

This is the most efficient and scalable solution for this use case.

B . Configure the switches to implement RADIUS accounting to HPE Aruba Networking ClearPass and enable HPE Aruba Networking ClearPass Insight:

Incorrect:

While ClearPass can provide visibility into user authentication and device activity, it is not specifically designed to detect or mitigate DoS attacks against switches.

C . Implement ARP inspection on all VLANs that support end-user devices:

Incorrect:

ARP inspection helps mitigate ARP spoofing or poisoning, but it does not directly address detection of DoS attacks like ICMP or ARP floods.

It is a preventative measure, not a detection tool.

D . Enabling debugging of security functions on the switches:

Incorrect:

Debugging logs can help troubleshoot specific issues but are not practical for real-time detection of DoS attacks.

Enabling debugging can overload the switch and is not suitable for proactive monitoring.

Final Recommendation

Deploying an NAE agent to monitor CoPP is the best solution because it provides real-time detection, alerting, and insights into traffic patterns that indicate DoS attacks.

Reference

AOS-CX Network Analytics Engine (NAE) Configuration Guide.

HPE Aruba AOS-CX Control Plane Policing Documentation.

Best Practices for Protecting Switches Against DoS Attacks in Aruba Networks.

Question: 90

A company has AOS-CX switches at the access layer, managed by HPE Aruba Networking Central. You have identified suspicious activity on a wired client. You want to analyze the client's traffic with Wireshark, which you have on your management station.

What should you do?

A. Access the client's switch's CLI from your management station. Access the switch shell and run a TCP dump on the client port.

B. Go to the client's switch in HPE Aruba Networking Central. Use the "Security" page to run a packet capture.

C. Set up a policy that implements a captive portal redirect to your management station. Apply that policy to the client's port.

D. Set up a mirror session on the client's switch; set the client port as the source and your station IP address as the tunnel destination.

Answer: D

Explanation:

Why a Mirror Session Is the Correct Choice

To analyze a wired client’s traffic with Wireshark, you need the traffic mirrored to your management station where Wireshark is installed. The most effective way to achieve this is by configuring a mirror session on the AOS-CX switch, specifying the client port as the source and your management station as the destination.

Analysis of Each Option

A . Access the client's switch's CLI from your management station. Access the switch shell and run a TCP dump on the client port:

Incorrect:

AOS-CX switches do not natively support packet capture (e.g., tcpdump) directly on the switch CLI.

This approach is not feasible for capturing and analyzing live client traffic.

B . Go to the client's switch in HPE Aruba Networking Central. Use the "Security" page to run a packet capture:

Incorrect:

HPE Aruba Networking Central provides security insights but does not directly support initiating packet captures for detailed analysis.

Traffic analysis with tools like Wireshark requires local packet capture at the management station.

C . Set up a policy that implements a captive portal redirect to your management station. Apply that policy to the client's port:

Incorrect:

Captive portals are designed for user authentication and redirection, not traffic analysis.

This would disrupt the client’s network activity without enabling traffic analysis in Wireshark.

D . Set up a mirror session on the client's switch; set the client port as the source and your station IP address as the tunnel destination:

Correct:

Mirroring the client port to your management station is the standard method for analyzing live network traffic with Wireshark.

Steps include:

Configure a mirror session on the client’s AOS-CX switch.

Set the client’s port as the source.

Set your management station as the destination using its IP address (via GRE tunnel or physical interface).

Start capturing traffic with Wireshark on the management station.

Final Recommendation

To analyze the client's traffic, configure a mirror session on the switch, set the client port as the source, and direct the traffic to your management station where Wireshark is running.

Reference

AOS-CX Switch Port Mirroring Configuration Guide.

HPE Aruba Networking Central Monitoring and Troubleshooting Best Practices.

Wireshark Traffic Analysis and Capture Techniques.

Question: 91

HPE Aruba Networking Central displays a Gateway Threat Count alert in the alert list. How can you gather more information about what caused the alert to trigger?

A. Use HPE Aruba Networking Central tools to run a Network Check on the gateway with which the alert is associated.

B. Use Live Monitoring on the gateway to download a packet capture of recent traffic flowing through the gateway.

C. Check the threat list for the gateway associated with the alert. Access threat details and download packet info.

D. Check the gateway's Audit Trail in HPE Aruba Networking Central for more details about the threats that triggered the alert.

Answer: C

Explanation:

Gateway Threat Count Alert

This alert indicates that the gateway has detected threats in traffic passing through it. HPE Aruba Networking Central provides tools to investigate and analyze these threats in detail.

Analysis of Each Option

A . Use HPE Aruba Networking Central tools to run a Network Check on the gateway with which the alert is associated:

Incorrect:

Network Check tools in Central are primarily used for connectivity and performance diagnostics, not for analyzing detected threats.

This does not provide insight into the specific threats triggering the Gateway Threat Count alert.

B . Use Live Monitoring on the gateway to download a packet capture of recent traffic flowing through the gateway:

Incorrect:

Live Monitoring and packet capture can provide raw traffic data, but interpreting this requires significant manual analysis.

The Gateway Threat Count alert already provides summarized threat insights that are easier to access via the threat list.

C . Check the threat list for the gateway associated with the alert. Access threat details and download packet info:

Correct:

The threat list is specifically designed to display detailed information about detected threats, such as their type, severity, and source/destination.

Administrators can access this list in Central for the affected gateway, view granular details, and even download associated packet data for deeper inspection.

D . Check the gateway's Audit Trail in HPE Aruba Networking Central for more details about the threats that triggered the alert:

Incorrect:

The Audit Trail tracks configuration changes and administrative actions, not the details of detected threats.

It is not relevant for investigating the Gateway Threat Count alert.

Final Recommendation

To gather more information about what caused the Gateway Threat Count alert to trigger, check the threat list for the associated gateway. This provides detailed threat information and the option to download packet data for further analysis.

Reference

HPE Aruba Networking Central Threat Management Guide.

Understanding Gateway IDS/IPS Alerts in Aruba Central Documentation.

Best Practices for Threat Investigation Using Aruba Central.

Question: 92

The following firewall role is configured on HPE Aruba Networking Central-managed APs:

wlan access-rule employees

index 3

rule any any match 17 67 67 permit

rule any any match any 53 53 permit

rule 10 5 5.0 255.255 255.0 match any any any deny

rule 10.5 0.0 255.255 0.0 match 6 80 80 permit

rule 10.5 0.0 255.255.0.0 match 6 443 443 permit

rule 10.5.0.0 255.255.0.0 match any any any deny

rule any any match any any any permit

A client has authenticated and been assigned to the employees role. The client has IP address 10.2.2.2. Which correctly describes behavior in this policy?

A. HTTPS traffic from 10.2.2.2 to 10.5.5.5 is denied.

B. HTTPS traffic from 10.2.2.2 to 203.0.113.12 is denied.

C. Traffic from 10.5.3.3 in an active HTTPS session between 10.2.2.2 and 10.5.3.3 is permitted.

D. Traffic from 198.51.100.12 in an active HTTP session between 10.2.2.2 and 198.51.100.12 is denied.

Answer: A

Explanation:

Policy Analysis:

Rule Evaluation Order: Rules are applied in sequential order until a match is found.

Key Points:

DHCP traffic (UDP 67) is permitted.

DNS traffic (UDP 53) is permitted.

Traffic to 10.5.5.0/24 is explicitly denied.

HTTP traffic (TCP 80) is allowed only to 10.5.0.0/16.

HTTPS traffic (TCP 443) is allowed only to 10.5.0.0/16.

All other traffic to 10.5.0.0/16 is denied.

Any other traffic not matching the above rules is permitted.

Scenario Analysis:

The client IP 10.2.2.2 does not fall within the 10.5.0.0/16 subnet.

Rule 3 denies traffic to 10.5.5.5, regardless of the source IP.

Option A: Correct. HTTPS traffic to 10.5.5.5 is explicitly denied by Rule 3.

Option B: Incorrect. Traffic to 203.0.113.12 is permitted due to the final "permit any" rule.

Option C: Incorrect. The client (10.2.2.2) does not belong to the subnet 10.5.0.0/16, so traffic to 10.5.3.3 is not permitted by Rule 5.

Option D: Incorrect. HTTP traffic to 198.51.100.12 is allowed by the last "permit any" rule.

Question: 93

You need to set up HPE Aruba Networking ClearPass Policy Manager (CPPM) to provide certificatebased authentication of 802.1X supplicants. How should you upload the root CA certificate for the supplicants' certificates?

A. As a ClearPass Server certificate with the RADIUS/EAP usage.

B. As a ClearPass Server certificate with the Database usage.

C. As a Trusted CA with the AD/LDAP usage.

D. As a Trusted CA with the EAP usage.

Answer: D

Explanation:

802.1 X Authentication Workflow: Requires the root CA certificate of the issuing authority for the supplicants' certificates. This ensures that the server can validate the client certificate during the EAP-TLS handshake.

Trusted CA Usage: In ClearPass, certificates with "Trusted CA" usage are used for validating client and server identities during secure authentication exchanges.

Option A: Incorrect. The "ClearPass Server certificate" is used for server-side identity verification and is not used to validate client certificates.

Option B: Incorrect. Database usage is unrelated to RADIUS/EAP or certificate validation.

Option C: Incorrect. While LDAP/AD integration supports certificate validation, this is not the primary purpose of Trusted CAs for 802.1X.

Option D: Correct. Trusted CAs for EAP are required to validate client certificates during the authentication process.

By uploading the root CA as a "Trusted CA with EAP usage," the CPPM can properly authenticate the certificates presented by the supplicants during EAP-TLS negotiations.

Question: 94

You are setting up policy rules in HPE Aruba Networking SSE. You want to create a single rule that permits users in a particular user group to access multiple applications. What is an easy way to meet this need?

A. Associate the applications directly with the IdP used to authenticate the users; choose any for the destination in the policy rule.

B. Apply the same tag to the applications; select the tag as a destination in the policy rule.

C. Place all the applications in the same connector zone; select that zone as a destination in the policy rule.

D. Select the applications within a non-default web profile; select that profile in the policy rule.

Answer: B

Explanation:

Tagging Applications: In HPE Aruba Networking SSE (Secure Service Edge), tagging is an efficient way to group multiple applications together for simplified management and rule creation.

Tags can be applied to applications, and a single policy rule can be configured to use the tag as the destination.

This eliminates the need to create multiple rules for each individual application, streamlining policy configuration.

Option B: Correct. Applying the same tag to multiple applications allows you to select the tag as the destination in a single policy rule, meeting the requirement efficiently.

Option A: Incorrect. Associating applications with the IdP and selecting "any" for the destination lacks granularity and security.

Option C: Incorrect. Using connector zones is more appropriate for network-level segmentation rather than grouping application policies.

Option D: Incorrect. Web profiles are generally used for web-based traffic policies, not for grouping applications in general.

Question: 95

A company has a variety of HPE Aruba Networking solutions, including an HPE Aruba Networking infrastructure and HPE Aruba Networking ClearPass Policy Manager (CPPM). The company passes traffic from the corporate LAN destined to the data center through a third-party SRX firewall. The company would like to further protect itself from internal threats. What is one solution that you can recommend?

A. Have the third-party firewall send Syslogs to CPPM, which can work with network devices to lock internal attackers out of the network.

B. Add ClearPass Device Insight (CPDI) to the solution, integrate it with the third-party firewall to develop more complete device profiles.

C. Configure CPPM to poll the third-party firewall for a broad array of information about internal clients, such as profile and posture.

D. Use tunnel mode SSIDs and user-based tunneling (UBT) on AOS-CX switches to pass all internal traffic directly through the third-party firewall.

Answer: A

Explanation:

Syslog Integration with CPPM:

ClearPass Policy Manager (CPPM) can integrate with third-party firewalls via Syslog messages to detect and respond to internal threats.

The Syslog integration enables CPPM to gather context on suspicious activity and enforce appropriate policies such as isolating attackers by working with network devices like Aruba switches and APs.

Option A: Correct. This method allows for dynamic response to threats and leverages existing infrastructure without requiring major reconfiguration.

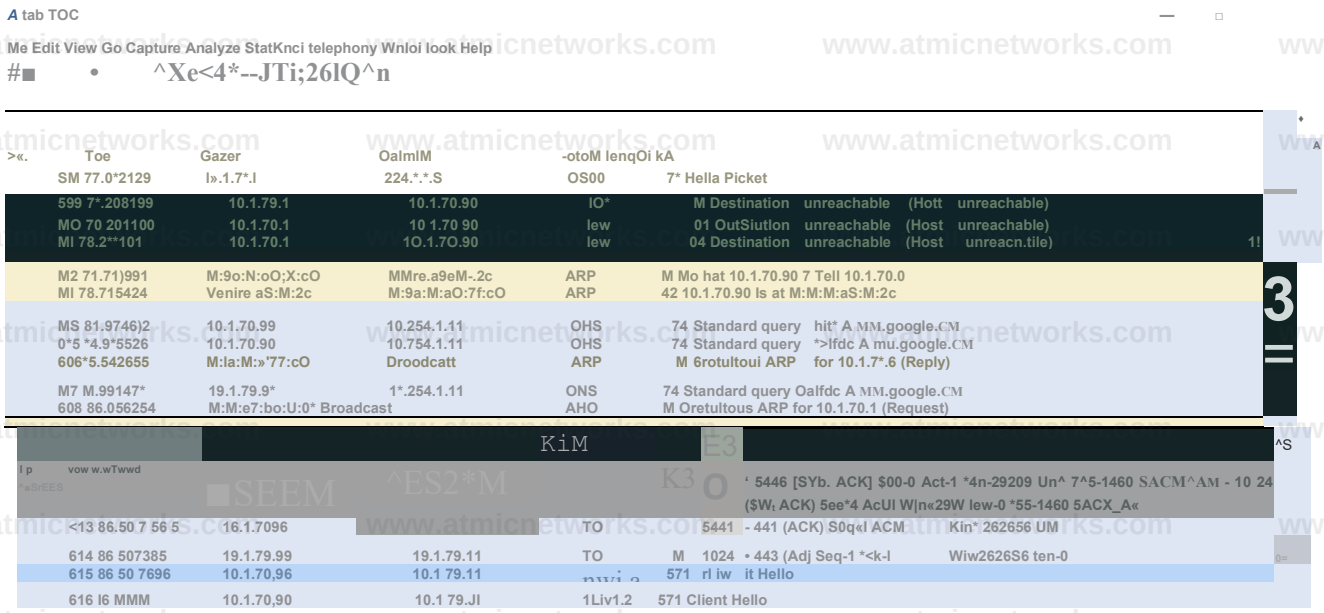
Option B: Incorrect. CPDI is primarily used for profiling devices, not directly for threat response based on Syslog information.

Option C: Incorrect. While it is possible for CPPM to poll information, this approach is less dynamic and not focused on immediate threat response.

Option D: Incorrect. Tunnel mode SSIDs and UBT are designed for forwarding user traffic securely but do not directly enhance threat detection or mitigation.

Question: 96

Refer to the exhibit.



The exhibit shows a saved packet capture, which you have opened in Wireshark. You want to focus on the complete conversation between 10.1.70.90 and 10.1.79.11 that uses source port 5448.

What is a simple way to do this in Wireshark?

A. Apply a capture filter that selects for both the 10.1.70.90 and 10.1.79.11 IP addresses.

B. Click the Source column and then the Destination column to sort the packets into the desired order.

C. Apply a capture filter that selects for TCP port 5448.

D. Right-click one of the packets between those addresses and choose to follow the stream.

Answer: D

Explanation:

Wireshark: Follow TCP Stream:

Wireshark provides an intuitive feature to filter and display a complete TCP conversation.

By right-clicking any packet within the conversation and selecting "Follow → TCP Stream", Wireshark isolates and displays the entire conversation.

This feature allows you to view the communication in a simplified, sequential manner, including requests and responses.

Option Analysis:

Option A: Incorrect. Capture filters only apply during packet capturing, not for analyzing already saved packet captures.

Option B: Incorrect. Sorting packets helps with organizing data but does not isolate a complete conversation.

Option C: Incorrect. A capture filter for TCP port 5448 would have to be applied before capturing; it does not work for saved data.

Option D: Correct. Right-clicking a packet and choosing "Follow TCP Stream" is the simplest way to display the full conversation between 10.1.70.90 and 10.1.79.11 on port 5448.

Steps in Wireshark to Follow a TCP Stream:

Locate any packet within the desired conversation (e.g., between 10.1.70.90 and 10.1.79.11 on TCP port 5448).

Right-click on the packet.

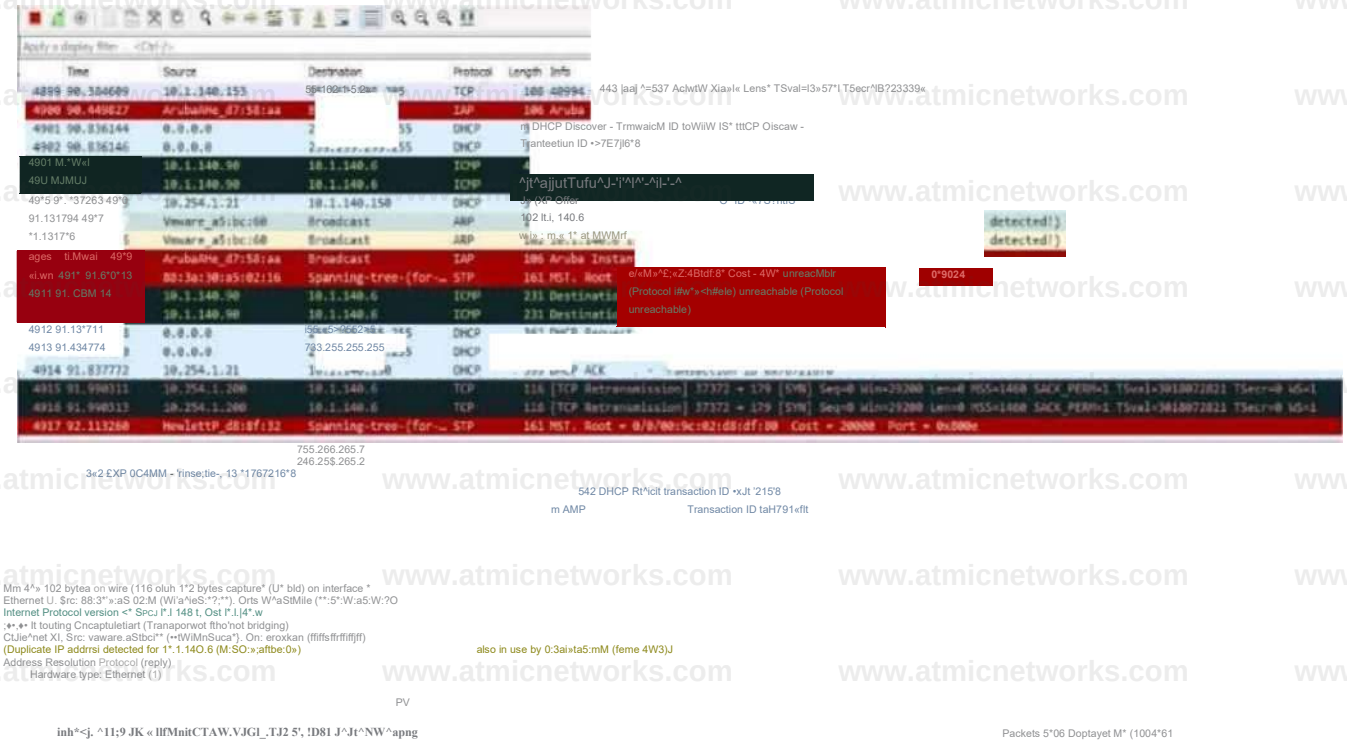
Choose "Follow" → "TCP Stream".

Wireshark will display the entire TCP conversation, including both directions of communication.

This feature is especially useful when troubleshooting or analyzing detailed interactions between hosts.

Question: 97

Refer to the Exhibit:



These packets have been captured from VLAN 10. which supports clients that receive their IP addresses with DHCP.

What can you interpret from the packets that you see here?

These packets have been captured from VLAN 10, which supports clients that receive their IP addresses with DHCP. What can you interpret from the packets that you see here?

A. Someone is possibly implementing a MAC spoofing attack to gain unauthorized access.

B. The mirroring session that captured the packets was likely misconfigured and captured duplicate traffic.

C. An admin has likely misconfigured two clients to use the same DHCP settings.

D. Someone is possibly implementing an ARP poisoning and MITM attack.

Answer: A

Explanation:

The exhibit reveals duplicate IP addresses detected for 10.1.140.6, associated with two different MAC addresses:

88:56:56:ab:c6:89

88:13:30:a3:02:00

Key observations:

Duplicate IP Address Detection:

The message "Duplicate IP address detected for 10.1.140.6" clearly indicates two devices claiming the same IP address.

This typically occurs when one device spoofs the MAC address of another device to intercept or disrupt traffic.

MAC Spoofing Context:

MAC spoofing is a tactic used to impersonate another device's hardware address to gain unauthorized access to a network.

By spoofing a legitimate IP-MAC pairing, an attacker can bypass security mechanisms or cause denial-of-service conditions.

Why the Other Options are Incorrect:

Option B (Mirroring Misconfigured): While mirroring misconfiguration can duplicate traffic, it does not lead to a "duplicate IP detected" alert.

Option C (Misconfigured DHCP): Misconfigurations usually result in DHCP conflicts, but they do not typically involve two different MAC addresses for the same IP.

Option D (ARP Poisoning/MITM): ARP poisoning involves falsified ARP tables, but it does not directly trigger duplicate IP address detection. Instead, ARP packets flood the network.

Conclusion:

The evidence strongly suggests MAC spoofing, as two different MAC addresses are claiming the same IP address (10.1.140.6). This behavior is typical of attempts to gain unauthorized access or disrupt network operations.

Question: 98

A company is using HPE Aruba Networking Central SD-WAN Orchestrator to establish a hub-spoke VPN between branch gateways (BGWs) at 1164 site and VPNCs at multiple data centers. What is part of the configuration that admins need to complete?

A. In VPNCs' groups, establish VPN pools to control which branches connect to which VPNCs.

B. In BGWs' and VPNCs' groups, create default IKE policies for the SD-WAN Orchestrator to use.

C. In BGWs' groups, select the VPNCs to which to connect in a DC preference list.

D. At the global level, create default IPsec policies for the SD-WAN Orchestrator to use.

Answer: C

Explanation:

Hub-Spoke VPN Configuration:

HPE Aruba Central SD-WAN Orchestrator enables hub-spoke topology where branch gateways (BGWs) connect to VPN concentrators (VPNCs) located at data centers.

A key step in configuring this is defining which VPNCs the BGWs will prefer for connectivity.

The DC Preference List is configured in the BGW groups to prioritize the data centers to which BGWs connect.

Option Analysis:

Option A: Incorrect. VPN pools control IP allocation, not which branches connect to VPNCs.

Option B: Incorrect. IKE policies define key exchange mechanisms but are not part of the connection preference process.

Option C: Correct. Admins configure a DC preference list in BGW groups to determine connectivity priorities with VPNCs.

Option D: Incorrect. IPsec policies define encryption parameters at a global level, but this is not specific to the hub-spoke connection configuration.

Question: 99

A company has HPE Aruba Networking APs running AOS-10 that connect to AOS-CX switches. The APs will:

Authenticate as 802.1X supplicants to HPE Aruba Networking ClearPass Policy Manager (CPPM)

Be assigned to the "APs" role on the switches

Have their traffic forwarded locally

What information do you need to help you determine the VLAN settings for the "APs" role?

A. Whether the switches are using local user-roles (LURs) or downloadable user-roles (DURs).

B. Whether the APs bridge or tunnel traffic on their SSIDs.

C. Whether the switches have established tunnels with an HPE Aruba Networking gateway.

D. Whether the APs have static or DHCP-assigned IP addresses.

Answer: B

Explanation:

Traffic Forwarding for APs:

In AOS-10, AP traffic forwarding can happen locally (bridged) or through tunnels to a gateway.

The VLAN settings on the "APs" role depend on whether the APs bridge the SSID traffic locally or forward it through a tunnel.

Option B: Correct. You need to know whether the traffic is bridged or tunneled to determine the VLAN assignments.

Option A: Incorrect. LURs/DURs affect role assignment but not VLAN settings for traffic forwarding.

Option C: Incorrect. Establishing tunnels with gateways is relevant to centralized traffic forwarding, not VLANs for bridged traffic.

Option D: Incorrect. AP IP addressing (static or DHCP) does not impact the VLAN for forwarded SSID traffic.

Question: 100

A company has AOS-CX switches, which authenticate clients to HPE Aruba Networking ClearPass Policy Manager (CPPM). CPPM is set up to receive a variety of information about clients' profile and posture. New information can mean that CPPM should change a client's enforcement profile. What should you set up on the switches to help the solution function correctly?

A. Enable RADIUS accounting to CPPM, including interim RADIUS accounting.

B. Configure a RADIUS track that references CPPM's FQDN or IP address.

C. Enable dynamic authorization, and specify CPPM as a dynamic authorization client.

D. Re-configure the authentication server on the switch specifying CPPM as a TACACS server.

Answer: C

Explanation:

Dynamic Authorization for Enforcement Profile Updates:

When CPPM receives updated client posture or profile data, it can initiate a Change of Authorization (CoA) to update enforcement profiles dynamically.

To support this:

Dynamic Authorization must be enabled on the switches.

CPPM must be configured as a dynamic authorization client to send CoA requests.

Option C: Correct. Dynamic authorization ensures that the switch can apply updated enforcement profiles based on new information from CPPM.

Option A: Incorrect. RADIUS accounting provides session updates but does not enable dynamic changes to enforcement profiles.

Option B: Incorrect. RADIUS track is for monitoring RADIUS server availability, not dynamic enforcement updates.

Option D: Incorrect. TACACS is not used for dynamic authorization; RADIUS handles this functionality.

Question: 101

A company already uses HPE Aruba Networking ClearPass Policy Manager (CPPM) as the RADIUS server for authenticating wireless clients with 802.1X. Now you are setting up 802.1X on AOS-CX switches to authenticate many of those same clients on wired connections. You decide to copy CPPM's wireless 802.1X service and then edit it with a new name and enforcement policy. What else must you change for authentication to work properly?

A. Role mapping policy

B. Authentication methods

C. Authentication source

D. Service rules

Answer: D

Explanation:

802.1 X Service Rules:

Service rules define the criteria for when a specific service applies (e.g., wireless vs. wired authentication).

For wired 802.1X authentication to work properly, the service rules need to differentiate between wireless and wired connections.

If you copy the wireless service, the rules likely still match wireless-specific criteria. These must be updated to include wired-specific conditions (e.g., NAS IP or port types).

Option Analysis:

Option A (Role mapping policy): Role mapping policies determine user roles based on attributes but are not critical for differentiating wired vs. wireless.

Option B (Authentication methods): Authentication methods (e.g., EAP) remain the same for both wireless and wired 802.1X.

Option C (Authentication source): Authentication sources (like AD or internal database) do not need to change.

Option D (Service rules): Correct. Updating the service rules ensures the new 802.1X service applies specifically to wired connections.

Question: 102

You are configuring the HPE Aruba Networking ClearPass Device Insight Integration settings on ClearPass Policy Manager (CPPM). For which use case should you set the 'Tag Updates Action" to "apply for all tag updates"?

A. When the Device Insight integration poll interval is set to a relatively long interval but you still want CPPM to be informed quickly about devices' new tags.

B. When Device Insight tags are only used to identify dangerous devices, and you want to disconnect those devices without having to set up new rules in enforcement policies.

C. When CPPM is gathering posture information for CPDI, and you want CPDI to always have access to the most up-to-date information.

D. When you plan to have CPPM issue CoAs for clients with new tags, but do not want to have to list those specific tags in the Device Integration settings in advance.

Answer: D

Explanation:

Tag Updates Action - "Apply for All Tag Updates":

This setting ensures that all updated tags from Device Insight (CPDI) are applied dynamically.

It is particularly useful when you want to trigger Change of Authorization (CoA) without explicitly predefining the tag values.

Option D: Correct. This setting allows CPPM to issue CoAs automatically for updated tags without requiring prior configuration of specific tags.

Option A: Incorrect. The setting is not directly related to reducing the poll interval latency.

Option B: Incorrect. Disconnecting devices based on dangerous tags would require predefined enforcement rules.

Option C: Incorrect. Posture information updates do not directly rely on this setting.

Question: 103

You are helping an organization deploy HPE Aruba Networking SSE. What is one reason to recommend that the company install agents on remote users' devices?

A. To run posture checks and apply different permissions based on those checks.

B. To permit admins to manage the HPE Aruba Networking SSE policy rules.

C. To permit users to access private servers using SSH.

D. To run threat inspection on clients in a local sandbox rather than in the cloud.

Answer: A

Explanation:

Installing Agents for SSE (Secure Service Edge):

Agents installed on remote users' devices allow posture checks (e.g., antivirus status, OS version) to ensure compliance.

Based on the results of the posture checks, different permissions and security policies can be applied dynamically.

This improves the security posture of remote users before granting access to resources.

Option A: Correct. Agents enable posture checks and enforce conditional access based on compliance.

Option B: Incorrect. Admins manage SSE policies centrally, not via agents.

Option C: Incorrect. Access to private servers via SSH does not require agents; it relies on policies and tunnels.

Option D: Incorrect. Local sandboxing is generally a function of endpoint protection solutions, not SSE agents.

Question: 104

You want to examine the applications that a device is using and look for any changes in application usage over several different ranges. In which HPE Aruba Networking solution can you view this information in an easy-to-view format?

A. HPE Aruba Networking ClearPass OnGuard agent installed on the device

B. HPE Aruba Networking Central within a device's Live Monitoring page

C. HPE Aruba Networking ClearPass Insight using an Active Endpoint Security report

D. HPE Aruba Networking ClearPass Device Insight (CPDI) in the device's network activity

Answer: B

Explanation:

HPE Aruba Central Live Monitoring:

Aruba Central provides real-time Live Monitoring of network devices, including:

Application usage statistics.

Trends and changes over time for specific devices.

This information is presented in a clear and easy-to-read format, making it ideal for examining changes in application usage over different time ranges.

Option Analysis:

Option A: Incorrect. ClearPass OnGuard monitors endpoint compliance (e.g., antivirus, OS version) but does not analyze application usage.

Option B: Correct. Aruba Central's Live Monitoring page is specifically designed for this type of analysis.

Option C: Incorrect. ClearPass Insight generates endpoint security reports but does not track application usage.

Option D: Incorrect. ClearPass Device Insight (CPDI) focuses on device profiling and identification, not continuous application monitoring.

Question: 105

A company wants to use HPE Aruba Networking ClearPass Policy Manager (CPPM) to profile Linux devices. You have decided to schedule a subnet scan of the devices' subnets. Which additional step should you complete before scheduling the scan?

A. Set up SSH accounts on CPPM and map them to the Linux devices' subnets.

B. Enable WMI probing in the cluster-wide parameters.

C. Enable the Data Port in the ClearPass server settings and connect that port to the network.

D. Configure SNMP in the network device settings for the switches that support the Linux devices.

Answer: C

Explanation:

Subnet Scan Requirements for Profiling:

For ClearPass to scan and profile devices in a subnet, the Data Port must be enabled on the ClearPass server and connected to the network.

This ensures that ClearPass can send and receive the required packets for device discovery and profiling.

Option Analysis:

Option A: Incorrect. SSH accounts are not required for subnet scanning.

Option B: Incorrect. WMI probing is for Windows systems, not Linux devices.

Option C: Correct. The Data Port is essential for subnet scans and must be properly configured and connected.

Option D: Incorrect. SNMP is used for network device monitoring, not Linux device profiling.

Question: 106

HPE Aruba Networking switches are implementing MAC-Auth to HPE Aruba Networking ClearPass Policy Manager (CPPM) for a company's printers. The company wants to quarantine a client that spoofs a legitimate printer's MAC address. You plan to add a rule to the MAC-Auth service enforcement policy for this purpose. What condition should you include?

A. Endpoint Compliance EQUALS false

B. Endpoint Device Insight Tag EXISTS

C. Authorization: [Endpoints Repository] Compromised EQUALS true

D. Authorization: [Endpoints Repository] Conflict EQUALS true

Answer: D

Explanation:

MAC Spoofing Detection with Endpoint Conflict:

When two devices attempt to use the same MAC address, ClearPass identifies a Conflict state in the Endpoints Repository.

This condition can be used to detect and quarantine clients that spoof legitimate devices.

Option D: Correct. The Conflict EQUALS true condition identifies devices with duplicate MAC addresses.

Option A: Incorrect. Endpoint compliance checks posture, not MAC spoofing.

Option B: Incorrect. Device Insight Tags are used for profiling but do not identify conflicts.

Option C: Incorrect. Compromised devices relate to security incidents, not MAC address conflicts.

Question: 107

A company wants to apply role-based access control lists (ACLs) on AOS-CX switches, which are implementing authentication to HPE Aruba Networking ClearPass Policy Manager (CPPM). The company wants to centralize configuration as much as possible. Which correctly describes your

options?

A. You can configure the role on CPPM; however, the CPPM role must reference a policy name that is configured on the switch.

B. You can configure the role name on CPPM; however, the role settings, including policy and classes, must be configured locally on the switch.

C. You can configure the role, its policy, and the classes referenced in the policy all on CPPM.

D. You can configure the role and its policy on CPPM; however, the classes referenced in the policy must be configured locally on the switch.

Answer: A

Explanation:

Centralized Role Configuration on CPPM:

CPPM can assign roles to clients dynamically during authentication.

However, the actual ACL policies (e.g., firewall policies) must already exist and be referenced locally on the switch.

CPPM cannot directly configure ACL details on AOS-CX switches.

Option Analysis:

Option A: Correct. The role is defined on CPPM, but it references a policy pre-configured on the switch.

Option B: Incorrect. This does not align with Aruba's centralized role-based access control design.

Option C: Incorrect. CPPM cannot configure the ACL policies and classes directly; they must exist locally.

Option D: Incorrect. Policies can be referenced centrally but not fully configured on CPPM.

Question: 108

A company has HPE Aruba Networking APs running AOS-10 and managed by HPE Aruba Networking Central. The company also has AOS-CX switches. The security team wants you to capture traffic from a particular wireless client. You should capture this client's traffic over a 15-minute time period and then send the traffic to them in a PCAP file. What should you do?

A. Access the CLI for the client's AP. Set up a mirroring session between its radio and a management station running Wireshark.

B. Go to the client's AP in HPE Aruba Networking Central. Use the "Security" page to run a packet capture.

C. Go to that client in HPE Aruba Networking Central. Use the "Live Events" page to run a packet capture.

D. Access the CLI for the client's AP's switch. Set up a mirroring session between the AP's port and a management station running Wireshark.

Answer: B

Explanation:

Packet Capture in Aruba Central:

Aruba Central provides tools for remote packet captures directly from the APs.

On the "Security" page for the AP, you can initiate a packet capture session, specifying the client device and capture duration.

The traffic is captured into a PCAP file, which can be downloaded and analyzed using tools like Wireshark.

Option Analysis:

Option A: Incorrect. While possible via CLI, Aruba Central provides a simpler method for packet captures.

Option B: Correct. Aruba Central's "Security" page allows you to capture and export client traffic efficiently.

Option C: Incorrect. The "Live Events" page focuses on monitoring events, not packet captures.

Option D: Incorrect. Port mirroring on the switch captures AP traffic but requires more manual configuration and does not isolate client-specific wireless traffic easily.

Question: 109

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. Enable Insight in the CPPM server configuration settings.

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

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

Answer: B

Explanation:

ClearPass Device Insight Integration:

To integrate ClearPass Device Insight (CPDI) with ClearPass Policy Manager (CPPM), you must enable the Insight feature in the CPPM server configuration settings.

This ensures CPPM can share and receive profiling data with CPDI for device identification.

Option Analysis:

Option A: Incorrect. Root CA certificates are not required for this integration.

Option B: Correct. Enabling Insight on CPPM is essential for the integration to function.

Option C: Incorrect. WMI, SSH, and SNMP are not part of the CPDI integration prerequisites.

Option D: Incorrect. The Data Collector token is relevant to Aruba Central, not CPDI integration.

Question: 110

A company wants you to create a custom device fingerprint on CPPM with rules for profiling a group of specialized devices. What is one requirement?

A. Connecting a known device of this type and getting it discovered in CPPM's Endpoints Repository.

B. Enabling HPE Aruba Networking ClearPass Device Insight integration with the correct Data Collector token.

C. Pre-defining the desired attributes and rules in an XML format file.

D. Disabling the "Automatically download Endpoint Profiler Fingerprints" feature in cluster-wide parameters.

Answer:
A

Explanation:

Custom Device Fingerprinting on CPPM:

To create a custom fingerprint, you first need to connect a known device of that type to the network.

CPPM will discover the device in its Endpoints Repository, allowing you to analyze its attributes (e.g., MAC OUI, DHCP options) and create custom profiling rules.

Option Analysis:

Option A: Correct. Discovering a known device in the Endpoints Repository is a prerequisite for creating accurate custom fingerprint rules.

Option B: Incorrect. CPDI integration is not required for custom fingerprints on CPPM.

Option C: Incorrect. XML rules are not pre-defined; they are created dynamically based on observed attributes.

Option D: Incorrect. The "Automatically download Endpoint Profiler Fingerprints" setting is unrelated to custom profiling.

Question: 111

Refer to the exhibit:

The exhibit shows the TACACS+ enforcement profile that HPE Aruba Networking ClearPass Policy

Manager (CPPM) assigns to a manager. When this manager logs into an AOS-CX switch, what does the switch do?

A. Assigns the manager operator-level privileges

B. Assigns the manager administrator-level privileges

C. Rejects the manager with an error message

D. Assigns the manager auditor-level privileges

Answer: A

Explanation:

TACACS+ Enforcement Profile:

The profile specifies a Service Attribute under Aruba:Common with:

Name: Aruba-Admin-Role

Value: operators

AOS-CX Role Mapping:

On Aruba AOS-CX switches, the Aruba-Admin-Role attribute maps the authenticated user to predefined roles:

operators: Operator-level privileges (read-only access, limited commands).

administrators: Full administrator privileges.

Other roles like auditors may exist based on configuration.

Analysis:

The value operators explicitly maps the user to operator-level privileges, granting read-only access to the AOS-CX switch.

Since the Aruba-Admin-Role is correctly set and recognized, the switch assigns the appropriate role without errors.

Option Breakdown:

Option A: Correct. The switch assigns operator-level privileges based on the Aruba-Admin-Role value.

Option B: Incorrect. Administrator-level privileges require the role value to be administrators.

Option C: Incorrect. The manager is successfully authenticated and authorized; there is no error.

Option D: Incorrect. There is no reference to an auditor role in the configuration shown.

Conclusion:

The operators value in the TACACS+ enforcement profile ensures that the manager is assigned operator-level privileges on the AOS-CX switch.

Question: 112

You are using Wireshark to view packets captured from HPE Aruba Networking infrastructure, but you're not sure that the packets are displaying correctly. In which circumstance does it make sense to configure Wireshark to ignore protection bits with the IV for the 802.11 protocol?

A. When the traffic was captured on the data plane of an HPE Aruba Networking gateway and sent to a remote IP.

B. When the traffic was mirrored from an AOS-CX switch port connected to an AP.

C. When the traffic was captured from an AP with HPE Aruba Networking Central.

D. When the traffic was captured on the control plane of an HPE Aruba Networking MC and sent to a remote IP.

Answer: C

Explanation:

802.11 Traffic and Protection Bits:

In the 802.11 protocol, protection bits and the Initialization Vector (IV) are used in encrypted wireless traffic.

If the traffic is captured directly from an AP, the frames may include encrypted content.

Wireshark may misinterpret these protection bits or fail to display the frames correctly unless it is configured to ignore protection bits and correctly parse the IV.

Key Scenario:

When traffic is captured directly from an AP managed by HPE Aruba Networking Central, the frames are often captured before decryption occurs.

In such cases, you must configure Wireshark to ignore the protection bits and handle the IV properly for correct frame interpretation.

Option Analysis:

Option A: Incorrect. Data plane traffic sent to a remote IP is usually decrypted, so Wireshark does not require this adjustment.

Option B: Incorrect. Switch port mirroring captures traffic at Layer 2/3, not raw 802.11 frames.

Option C: Correct. Traffic captured directly from an AP via HPE Aruba Networking Central often includes encrypted wireless frames, requiring Wireshark adjustments.

Option D: Incorrect. Control plane traffic is typically management data and not raw wireless frames needing IV interpretation.

Question: 113

You have enabled "rogue AP containment" in the Wireless IPS settings for a company's HPE Aruba Networking APs. What form of containment does HPE Aruba Networking recommend?

A. Wireless deauthentication only

B. Wireless tarpit and wired containment

C. Wireless tarpit only

D. Wired containment

Answer: A

Explanation:

Rogue AP Containment Methods:

HPE Aruba Networking recommends using wireless deauthentication as the preferred method for rogue AP containment.

Deauthentication sends deauth frames to clients connected to rogue APs, causing them to disconnect. This method is effective without introducing unnecessary disruptions to the wired infrastructure.

Key Points:

Wireless Deauthentication is simple, efficient, and widely supported across client devices.

Tarpit Containment is more aggressive and may cause unintentional disruptions to legitimate clients.

Wired Containment involves blocking traffic at the switch level but is complex and may impact legitimate infrastructure traffic.

Option Analysis:

Option A: Correct. Wireless deauthentication is the recommended method as it targets rogue AP clients without excessive network impact.

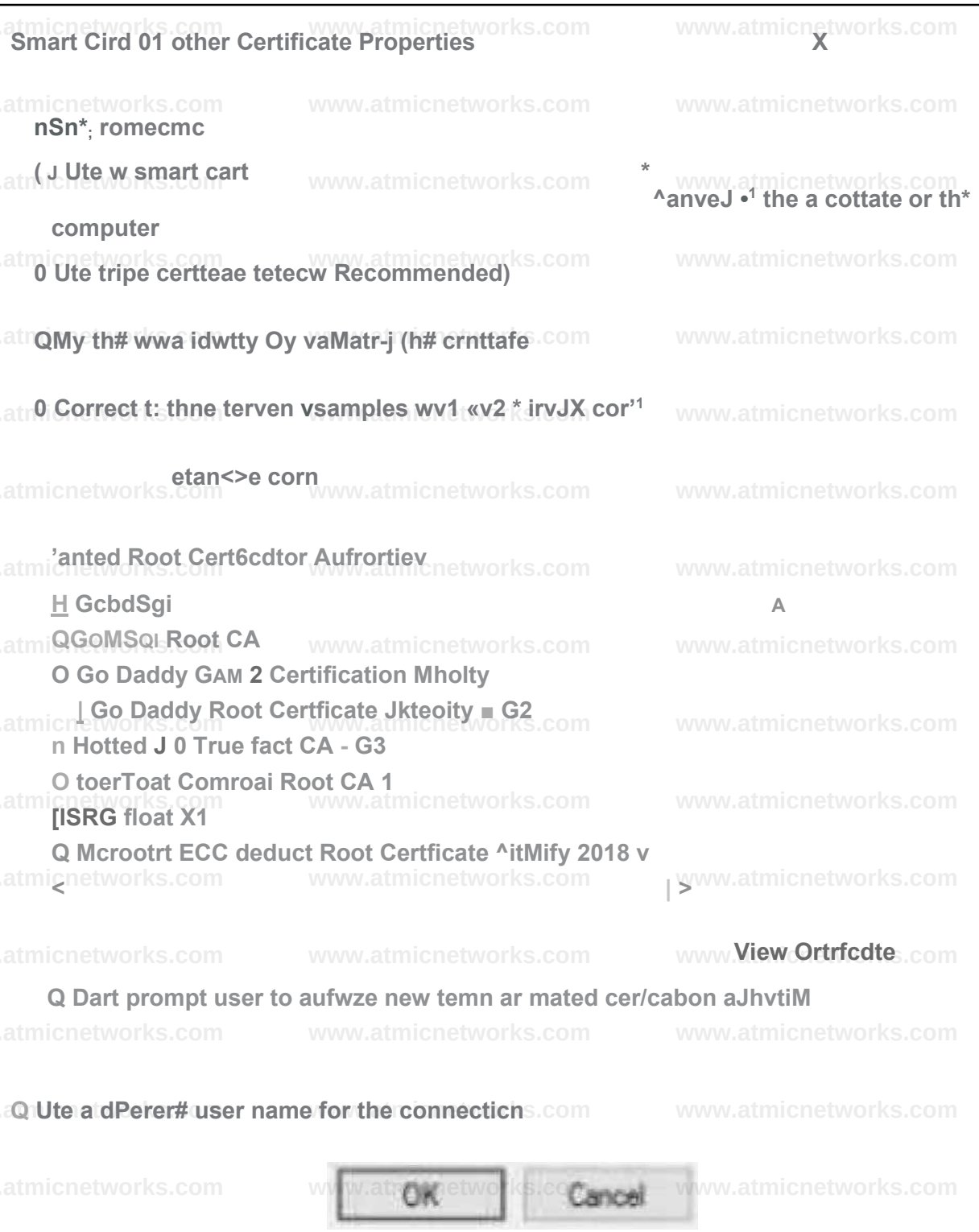
Option B: Incorrect. Combining wireless tarpit and wired containment is overkill and not typically recommended.

Option C: Incorrect. Wireless tarpit can be effective but is generally not the first choice due to its aggressive nature.

Option D: Incorrect. Wired containment is more complex and reserved for specific use cases, not general recommendations.

Question: 114

Refer to the exhibit.



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: A

Explanation:

To follow best security practices for 802.1X authentication settings in Windows domain clients:

Specify at least two server names under "Connect to these servers":

Admins should explicitly list trusted RADIUS server names (e.g., radius.example.com) to prevent the client from connecting to unauthorized or rogue servers.

This mitigates man-in-the-middle (MITM) attacks where an attacker attempts to present their own RADIUS server.

Select the desired Trusted Root Certificate Authority and "Don't prompt users":

Select the Trusted Root CA that issued the RADIUS server's certificate. This ensures clients validate the correct server certificate during the EAP-TLS/PEAP authentication process.

Enabling "Don't prompt users" ensures end users are not confused or tricked into accepting certificates from untrusted servers.

Why the other options are incorrect:

Option C: Incorrect. Wildcards in server names (e.g., *.example.com) weaken security and allow broader matching, increasing the risk of rogue servers.

Option D: Incorrect. Clearing "Use simple certificate selection" requires users to select certificates manually, which can lead to errors and usability issues. Simple certificate selection is recommended when properly configured.

Recommended Settings for Best Security Practices:

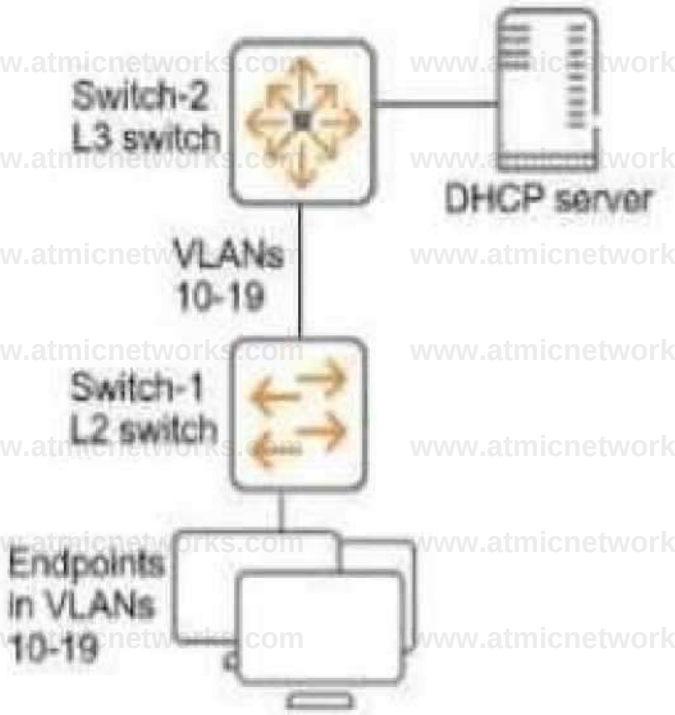
Server Validation: Specify the exact RADIUS server names in the "Connect to these servers" field.

Root CA Validation: Ensure only the correct Trusted Root Certificate Authority is selected.

User Prompts: Enable "Don't prompt users" to enforce automatic and secure authentication without user intervention.

Question: 115

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?

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: 116

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?

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:

802.1 X 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.

Question: 117

You need to create a rule in an HPE Aruba Networking ClearPass Policy Manager (CPPM) role mapping policy that references a ClearPass Device Insight Tag. Which Type (namespace) should you specify for the rule?

A. Endpoint

B. TIPS

C. Device

D. Application

Answer: A

Explanation:

ClearPass Role Mapping Policy:

The Endpoint namespace is used to reference attributes and tags related to endpoint devices.

Device Insight Tags are part of endpoint profiling information and are stored in the Endpoint Repository.

Option Analysis:

Option A: Correct. The Endpoint namespace includes Device Insight Tags.

Option B: Incorrect. TIPS refers to system attributes and configuration data, not endpoint tags.

Option C: Incorrect. Device is not a valid namespace in this context.

Option D: Incorrect. Application relates to application-level attributes, not Device Insight Tags.

Question: 118

What is one benefit of integrating HPE Aruba Networking ClearPass Policy Manager (CPPM) with third-party solutions such as Mobility Device Management (MDM) and firewalls?

A. CPPM can exchange contextual information about clients with third-party solutions, which helps make better decisions.

B. CPPM can make the third-party solutions more secure by adding signature-based threat detection capabilities.

C. CPPM can ofload policy decisions to the third-party solutions, enabling CPPM to respond to authentication requests more quickly.

D. CPPM can take over filtering internal traffic so that the third-party solutions have more processing power to devote to filtering external traffic.

Answer: A

Explanation:

Contextual Exchange for Better Decisions:

HPE Aruba ClearPass can integrate with third-party solutions like MDM and firewalls to exchange contextual information about endpoints (e.g., device type, posture, location).

This integration allows ClearPass and the third-party solutions to make better access control and security decisions.

For example:

An MDM can inform CPPM about device compliance, and CPPM can adjust enforcement policies dynamically.

Firewalls can receive updated context about users and devices to enforce policies more effectively.

Option Analysis:

Option A: Correct. Exchanging contextual information improves access control decisions.

Option B: Incorrect. CPPM does not provide signature-based threat detection.

Option C: Incorrect. CPPM does not ofload policy decisions; it integrates for collaboration.

Option D: Incorrect. CPPM does not replace third-party traffic filtering capabilities.

Question: 119

You have created a Web-based Health Check Service that references a posture policy. You want the service to trigger a RADIUS change of authorization (CoA) when a client receives a Healthy or Quarantine posture. Where do you configure those rules?

A. In a RADIUS enforcement policy

B. In the Agents and Software Updates > OnGuard Settings

C. In the posture policy

D. In a WEBAUTH enforcement policy

Answer: A

Explanation:

RADIUS Change of Authorization (CoA):

CoA is triggered when ClearPass determines that a client's posture status has changed (e.g., Healthy, Quarantine).

The RADIUS enforcement policy is where you configure actions and enforcement profiles that respond to these posture changes.

Option Analysis:

Option A: Correct. RADIUS enforcement policies are used to configure actions, including triggering CoA.

Option B: Incorrect. OnGuard settings configure posture agent behavior, not enforcement rules.

Option C: Incorrect. The posture policy evaluates compliance but does not trigger CoA.

Option D: Incorrect. WEBAUTH enforcement policies are for web-based authentication, not posture- related CoA.

Question: 120

You have configured an AOS-CX switch to implement 802.1X on edge ports. Assume ports operate in the default auth-mode. VoIP phones are assigned to the "voice" role and need to send traffic that is tagged for VLAN 12. Where should you configure VLAN 12?

A. As the trunk native VLAN on edge ports and the trunk native VLAN on the "voice" role.

B. As the allowed trunk VLAN in the "voice" role (and not in the edge port settings).

C. As a trunk allowed VLAN on edge ports and the trunk native VLAN in the "voice" role.

D. As the trunk native VLAN in the "voice" role (and not in the edge port settings).

Answer: B

Explanation:

Voice Role VLAN Configuration:

When VoIP phones are authenticated and assigned to the "voice" role, VLAN 12 should be explicitly defined as an allowed trunk VLAN within the role configuration.

The VLAN configuration should be role-specific rather than on the edge port, as this ensures dynamic VLAN assignment based on authentication results.

Option Analysis:

Option A: Incorrect. Native VLANs are for untagged traffic, but VoIP traffic is tagged.

Option B: Correct. VLAN 12 must be configured as the allowed trunk VLAN in the "voice" role to tag VoIP traffic correctly.

Option C: Incorrect. Configuring VLAN 12 in both edge port and role settings is redundant and unnecessary.

Option D: Incorrect. Native VLANs do not handle tagged traffic like VLAN 12 for VoIP phones.

Question: 121

A company has AOS-CX switches and HPE Aruba Networking ClearPass Policy Manager (CPPM). The company wants switches to implement 802.1X authentication to CPPM and download user roles.

What is one task that you must complete on CPPM to support this use case?

A. Export roles on CPPM to a file that uses XML format.

B. Create an admin account for the switch on CPPM with the HPE Aruba Networking User Role Download privilege level.

C. Configure RADIUS enforcement profiles that specify the HPE-User-Role VSA.

D. Upload the switch TPM certificate as a trusted CA certificate with the Others usage.

Answer: C

Explanation:

802.1X and User Role Download:

AOS-CX switches use RADIUS attributes to dynamically download user roles from CPPM.

The HPE-User-Role VSA (Vendor-Specific Attribute) must be configured in the RADIUS enforcement profiles to specify which role the switch should apply.

Option Analysis:

Option A: Incorrect. Exporting roles in XML is not needed for dynamic role download.

Option B: Incorrect. Switches authenticate via RADIUS, not admin accounts with specific privileges.

Option C: Correct. RADIUS enforcement profiles must include the HPE-User-Role VSA to implement user role download.

Option D: Incorrect. TPM certificates are unrelated to RADIUS-based user role downloads.

Question: 122

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?

A. 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.

B. CPDI can use tags to inform CPPM that clients are using prohibited applications. CPPM can then tell the network infrastructure to quarantine those clients.

C. CPPM can provide CPDI with custom device fingerprint definitions in order to enhance the company's total visibility.

D. CPDI can provide CPPM with extra information about users' identity. CPPM can then use that information to apply the correct identity-based enforcement.

Answer: B

Explanation:

Integration of CPDI and CPPM for Zero Trust:

CPDI (ClearPass Device Insight) identifies and profiles devices and applications on the network.

CPDI can tag devices based on their behavior or detected applications.

CPPM uses these tags to enforce policies, such as quarantining clients that violate security rules (e.g., using prohibited applications).

Option Analysis:

Option A: Incorrect. CPPM does not inform CPDI about role assignments; CPDI provides device context to CPPM.

Option B: Correct. CPDI tags clients, and CPPM uses those tags to enforce quarantine or other Zero Trust actions.

Option C: Incorrect. Custom fingerprint definitions are not part of this integration.

Option D: Incorrect. CPDI provides information about devices, not user identities.

Question: 123

A company has HPE Aruba Networking infrastructure devices. The devices authenticate clients to HPE Aruba Networking ClearPass Policy Manager (CPPM). You want CPPM to track information about clients, such as their IP addresses and their network bandwidth utilization. What should you set up on the network infrastructure devices to help that happen?

A. Logging with CPPM configured as a Syslog server.

B. Dynamic authorization enabled in the RADIUS settings for CPPM.

C. RADIUS accounting to CPPM, including interim updates.

D. An IF-MAP interface with CPPM as the destination.

Answer: C

Explanation:

RADIUS Accounting:

RADIUS accounting enables network devices to report client session details (e.g., IP addresses, session duration, bandwidth usage) to CPPM.

Interim updates ensure CPPM receives ongoing updates about the client's session, enabling accurate tracking.

Option Analysis:

Option A: Incorrect. Syslog logging sends general system logs, not client session details.

Option B: Incorrect. Dynamic authorization (CoA) handles session changes but does not provide usage tracking.

Option C: Correct. RADIUS accounting with interim updates tracks client IP addresses and bandwidth utilization.

Option D: Incorrect. IF-MAP interfaces are used for metadata sharing, not for RADIUS-based tracking.

Question: 124

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:

RAPIDS Ad-Hoc Detection:

The alert "Detect ad-hoc using Valid SSID" indicates that a device is broadcasting an SSID that matches a valid network SSID in ad-hoc mode. This can be an indication of an infrastructure attack or misconfiguration.

Next Steps:

Use Aruba Central floorplans or AP location data to identify the physical area where the offending device is detected.

Locate and investigate the device to determine if it is malicious or simply misconfigured.

Option Analysis:

Option A: Incorrect. While tuning thresholds is useful for reducing false positives, this step does not directly address a potential threat.

Option B: Incorrect. Faulty drivers can cause similar behavior, but this step is not immediately actionable without locating the device first.

Option C: Correct. Floorplans or AP identities help locate the threat's physical area for further investigation.

Option D: Incorrect. RAPIDS focuses on detecting devices via SSID and MAC, not IP addresses, making this approach less relevant.

Question: 125

An AOS-CX switch has been configured to implement UBT to two HPE Aruba Networking gateways that implement VRRP on the users' VLAN. What correctly describes how the switch tunnels UBT users' traffic to those gateways?

A. The switch always sends the users' traffic to the VRRP master.

B. The switch always sends all users' traffic to the primary gateway configured in the UBT zone.

C. The switch always load shares the users' traffic across both gateways.

D. The switch always sends all users' traffic to the gateway assigned as the active device designed gateway.

Answer: B

Explanation:

User-Based Tunneling (UBT) with VRRP:

UBT allows traffic from authenticated users to be tunneled to an HPE Aruba Networking gateway.

In the case of VRRP, where two gateways are configured for redundancy, the AOS-CX switch will always send the traffic to the primary gateway defined in the UBT zone configuration.

The VRRP state (master/backup) does not impact the UBT decision; the UBT primary configuration takes precedence.

Option Analysis:

Option A: Incorrect. UBT does not strictly follow the VRRP master; it adheres to the UBT primary gateway configuration.

Option B: Correct. The switch tunnels all traffic to the primary gateway configured in the UBT zone.

Option C: Incorrect. UBT does not load-share traffic between gateways.

Option D: Incorrect. UBT uses the primary gateway configured in the UBT zone, not dynamically determined active devices.

Question: 126

A company wants HPE Aruba Networking ClearPass Policy Manager (CPPM) to periodically poll Microsoft Endpoint Manager (formerly Intune) for attributes about its managed clients.

What should you do on ClearPass to permit this integration?

A. Install the Intune extension from ClearPass Guest

B. Import the Intune dictionary into the ClearPass dictionaries

C. Create an Intune authentication source on CPPM

D. Configure Endpoint Manager (Intune) as an event source on CPPM

Answer: C

Explanation:

For ClearPass to periodically query Microsoft Intune / Endpoint Manager for device attributes (compliance, owner, OS, etc.), you must configure Intune as an authentication source in Policy Manager. The ClearPass–Intune integration is implemented through an API-based auth source which CPPM polls on a schedule; it is not done via Guest extensions or syslog/event sources.

Aruba's Intune integration guides describe configuring a "Microsoft Intune" (or "Endpoint Manager") authentication source in ClearPass and supplying the Azure app registration details so CPPM can poll Intune via Microsoft Graph.

Option A is incorrect: the Intune integration is not a ClearPass Guest extension.

Option B is insufficient: adding dictionaries only defines attributes; it does not enable scheduled polling.

Option D is incorrect: Intune is not used as a syslog/event source for this use case; ClearPass initiates the polling via the authentication source.

Therefore, the correct configuration step is: Create an Intune authentication source on CPPM (Option C).

Question: 127

You manage AOS-10 APs with HPE Aruba Networking Central. A role is configured on these APs with these rules (in order):

Allow UDP on port 67 to any destination

Allow any to network 10.1.4.0/23

Deny any to network 10.1.0.0/18 + log

Deny any to network 10.0.0.0/8

Allow any to any destination

You add this new rule immediately before rule 4:

Deny SSH to network 10.1.0.0/21 + denylist

After this change, what happens when a client assigned to this role sends SSH traffic to 10.1.7.12?

A. The traffic is permitted

B. The traffic is dropped and logged

C. The traffic is dropped, and the client is denylisted

D. The traffic is dropped (without any logging or further action against the client)

Answer: B

Explanation:

Aruba firewall / role access rules are evaluated top-down, first-match wins; once a rule matches, no later rules are processed.

Let's walk the packet through t⇒he ordered rules:

The traffic is SSH, not UDP/67 rule 1 doe⇒s not match.

Destination 10.1.7.12 is n o⇒t in 10.1.4.0/23 rule 2 does not match.

E. .1.7.12 is in 10.1.0.0/18 rule 3 matches first.

Rule 3 action: Deny any to 10.1.0.0/18 + log.

Because rule 3 already matched, the later "Deny SSH to 10.1.0.0/21 + denylist" rule is never evaluated, so no denylist is applied.

Aruba documentation for session ACLs and firewall rules explicitly states that rules are evaluated from top to bottom and "the first match terminates further evaluation," and logging/denylist flags on a rule are applied only when that specific rule matches.

So the outcome is: the SSH traffic is dropped and logged, but the client is not denylisted → Option B.

Question: 128

A company has HPE Aruba Networking APs and AOS-CX switches. The APs bridge wireless traffic. They receive DHCP IP addresses on VLAN 18. Wireless users are assigned to VLAN 12.

The company wants the APs to start using 802.1X authentication on their switch ports. You are configuring the port-access role to which the APs are assigned after authentication.

What is one recommended setting for that role?

A. No trust for DSCP

B. Trust for DSCP

C. Auth-mode left at client-mode

D. Access VLAN 18 with no support for VLAN 12

Answer: B

Explanation:

When a switch port connects to a wireless AP that bridges multiple client VLANs, best practice is to:

Keep the VLAN/trunking configuration on the interface (not forced by the role), so that both VLAN 18 (AP management) and VLAN 12 (clients) are supported.

Enable trust of DSCP on the AP uplink so that QoS markings from the AP (voice, real-time traffic) are honored end-to-end, instead of being remarked or reset at the switch. Aruba wired-access and campus deployment guides repeatedly recommend trusting DSCP on AP uplinks so that WMM/802.11e markings are preserved.

Option D ("Access VLAN 18 with no support for VLAN 12") would break the design because the AP needs to carry client VLAN 12 across its uplink. Option C (auth-mode client-mode) is about how many supplicants per port are authenticated; it is not the key "recommended" setting in this scenario, and

Aruba designs typically focus QoS for AP uplinks via trust settings.

Therefore, the recommended role setting here is to trust DSCP on the AP's authenticated role → Option B.

Question: 129

You are setting up HPE Aruba Networking SSE to detect threats as remote users browse the internet.

What is part of this process?

A. Creating a non-default file security profile

B. Integrating HPE Aruba Networking SSE with a supported third-party antivirus provider

C. Deploying a connector that can reach the remote users

D. Creating an external web profile that enables SSL inspection

Answer: D

Explanation:

HPE Aruba Networking SSE is a cloud-delivered Security Service Edge platform that provides secure web gateway, ZTNA, CASB/DLP, and cloud firewall functions. Threat detection for remote web browsing relies heavily on full traffic inspection, including SSL inspection, URL filtering, and malware scanning.

In Aruba SSE deployments that protect web access from campus/branch or remote users, you:

Integrate the on-prem gateway or AOS-10 environment with SSE using an external web profile, which defines how traffic is sent to SSE.

Within that profile, you enable SSL inspection so that SSE can decrypt and inspect HTTPS traffic, allowing advanced threat detection, DLP, and malware scanning.

Option A: Custom file security profiles can tune malware scanning, but using a non-default profile is not mandatory for basic threat detection.

Option B: SSE already includes built-in anti-malware and sandboxing; it doesn't require a separate third-party antivirus integration for core features.

Option C: Connectors in SSE are used mainly to reach private applications (ZTNA), not to "reach remote users" for general web browsing.

Therefore, an essential part of enabling threat detection for web browsing is creating an external web profile that enables SSL inspection → Option D.

Question: 130

You are proposing HPE Aruba Networking ZTNA to an organization that currently uses a third-party, IPsec-based client-to-site VPN.

What is one advantage of ZTNA that you should emphasize?

A. ZTNA improves security for SaaS applications, which now make up the majority of remote user traffic.

B. ZTNA offers no greater security than the current solution, but it makes it much easier for admins to create and maintain consistent policies.

C. ZTNA is specifically designed to enhance security for Internet of Things (IoT) devices, which traditional client-to-site VPNs cannot address.

D. ZTNA shrinks the attack surface, eliminating publicly exposed ports and reducing the extent of the private network exposed to remote users.

Answer: D

Explanation:

HPE Aruba Networking ZTNA (delivered as part of Aruba SSE) replaces traditional network-level VPN access with application-level access. Key security advantages highlighted in Aruba ZTNA/SSE collateral include:

Applications are no longer exposed directly to the internet; instead, they are fronted by the ZTNA service.

Inbound connectivity to private apps is outbound-only via connectors, eliminating open listening ports and shrinking the external attack surface. www6.h3c.com

Users are granted access only to specific applications, not entire subnets, thereby limiting lateral movement and the blast radius of a compromise.

Aruba documentation explicitly notes that ZTNA "reduces the overall attack surface" and avoids the broad network exposure inherent in classic client-to-site VPNs.

Thus, the most accurate advantage is: ZTNA shrinks the attack surface, eliminating publicly exposed ports and reducing the extent of the private network exposed to remote users → Option D.

Question: 131

You are using Wireshark to view packets captured from HPE Aruba Networking infrastructure, but you are not sure that the packets are displaying correctly.

In which circumstance does it make sense to ensure that Wireshark has GRE enabled as one of its analyzed protocols?

A. When the traffic was captured on an HPE Aruba Networking gateway and sent to a remote IP

B. When the traffic was captured on an HPE Aruba Networking gateway dataplane and saved to a file

C. When the traffic was captured on an HPE Aruba Networking Mobility Controller (MC) control plane and saved to a file

D. When the traffic was captured on an HPE Aruba Networking MC dataplane and saved to a file

Answer: D

Explanation:

On Aruba Mobility Controllers, dataplane captures can include wireless frames encapsulated inside GRE (for example, ERM / remote mirroring or tunneled 802.11 data). If Wireshark does not have GRE dissection enabled, these packets may appear as generic IP/UDP payloads, and the inner traffic (client frames) will not decode correctly.

MC dataplane is exactly where GRE-encapsulated user traffic is likely to appear. Enabling GRE in Wireshark allows you to see and decode the inner payload (802.11/Ethernet/IP).

MC control plane traffic is generally not GRE encapsulated data traffic.

For gateways, captures exported as ERM over UDP often require different decoding (e.g., ARUBA_ERM, not generic GRE).

Thus, the most appropriate case to ensure GRE is enabled is when the capture came from the MC dataplane → Option D.

Question: 132

What is one use case that companies can fulfill using HPE Aruba Networking ClearPass Policy Manager's (CPPM's) Device Profiler?

A. Applying the correct enforcement profiles to specialized clients such as security cameras

B. Identifying OS, browser, and application vulnerabilities by CVE ID

C. Authenticating clients to Active Directory computer accounts

D. Quarantining and remediating devices that have disabled firewalls

Answer: A

Explanation:

ClearPass Device Profiler gathers information (DHCP, HTTP user-agent, MAC OUI, RADIUS, etc.) to identify device types and roles—especially non-user devices. Aruba documentation describes using profiling to recognize and categorize devices such as IP cameras, printers, and IoT "bots", and to supply this identity context to access control

policies. ExamTopics

Typical use cases include:

Automatically identifying a device as a security camera, printer, IP phone, etc.

Using that profile to assign an appropriate role/VLAN and enforcement profile in CPPM (e.g., restricted video-surveillance VLAN).

ClearPass literature explicitly calls out that Device Profiler is used to "automatically profile devices and provide an identity context (such as cameras, printers, or bots)" that can be used in policy decisions.

Options B, C, and D are handled by vulnerability scanners, directory services, or posture/OnGuard, not by Device Profiler itself. Therefore the correct use case is Option A.

Question: 133

A company wants to use the HPE Aruba Networking ClearPass OnGuard agent to assign posture to clients.
How do you define the conditions by which a client receives a particular posture?

A. Create rules within a posture policy

B. Create rules within a WebAuth enforcement policy

C. Create the rules directly in a service's Enforcement tab

D. Create rules directly in a service's Posture tab

Answer: A

Explanation:

ClearPass OnGuard uses a Posture Policy object to define:

Which checks are performed (e.g., AV installed, firewall status, patches)

How the results map to posture tokens such as "Healthy," "Quarantined," etc.

The official OnGuard configuration workflow states that you must first "Define the posture policy", and that these posture policies contain the rules for evaluating health and determining posture tokens.

Service enforcement policies then consume the posture token (e.g., Tips:Posture = Healthy) but do not define the posture conditions themselves. The "Posture" tab on a service is used to enable posture and associate it with the posture policy; the detailed rules live in the posture policy object.

Therefore, posture logic is defined by creating rules within a posture policy → Option A.

Question: 134

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:

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: 135

As part of setting up an HPE Aruba Networking ClearPass Onboard solution for wireless clients, you created Network Settings, a Configuration Profile, and a Provisioning Settings object in ClearPass Onboard. You also ran the ClearPass Onboard Service Only Template on ClearPass Policy Manager (CPPM).

You now need to ensure that only domain users are authenticated and allowed to log into the ClearPass Onboard portal.

Which component should you edit?

A. The Network Settings on ClearPass Onboard

B. The ClearPass Onboard Service Pre-Auth service on CPPM

C. The 802.1X services on CPPM used for wireless clients

D. The Provisioning profile on ClearPass Onboard

Answer: B

Explanation:

Access to the Onboard portal is controlled by a dedicated Pre-Auth service in ClearPass Policy Manager:

The "ClearPass Onboard Service Pre-Auth" service defines which authentication sources (e.g., AD domain, local DB, guest) are used when users log into the Onboard web portal.

To restrict access to domain users only, you edit this Pre-Auth service to use only the Active Directory auth source (and appropriate authorization checks, such as group membership).

Exam and configuration references for ClearPass Onboard clearly identify the Onboard Pre-Auth service as the place where you control who can log into the Onboard portal.

Network Settings and Provisioning profiles in Onboard govern SSID, profiles, and device configuration, not portal user authentication.

The 802.1X services for wireless control network access after onboarding, not login to the onboarding portal itself.

Therefore, to limit the portal to domain users, you should edit the ClearPass Onboard Service Pre- Auth service on CPPM → Option B.