Number: HPE7-A02
Passing Score: 800
Time Limit: 120
File Version: 3.0

Exam Code: HPE7-A02

Exam Name: Aruba Certified Network Security Professional

Exam A

QUESTION 1
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

Correct Answer: B
Section:
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.

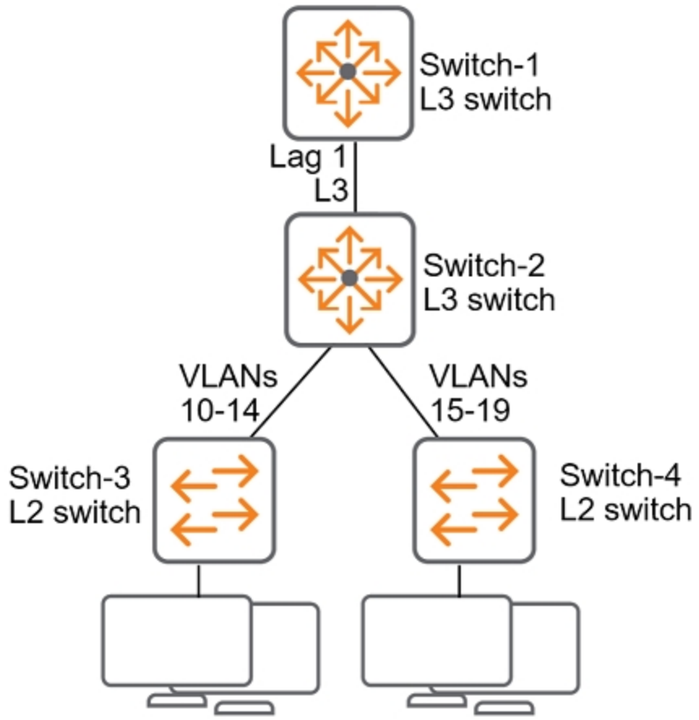
QUESTION 2
A company uses HPE Aruba Networking ClearPass Device Insight (CPDI) (the standalone application option). In the details for a generic device cluster, you see a recommendation for 'Windows 8/10' with 70% accuracy.
What does this mean?

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.

Correct Answer: A
Section:
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.

QUESTION 3
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.

Correct Answer: C
Section:
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.

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'

Correct Answer: D
Section:
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.

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.

Correct Answer: B
Section:
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.

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 Internet-facing 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.

Correct Answer: A
Section:
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.

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.'

Correct Answer: B
Section:
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.

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

Correct Answer: D
Section:
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.

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.

Correct Answer: A
Section:
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.

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

Correct Answer: A
Section:
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.

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.

Correct Answer: A
Section:
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.

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

Correct Answer: D
Section:
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.

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.

Correct Answer: A
Section:
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.

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

Correct Answer: B
Section:
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.

QUESTION 15
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. Configure all edge ports in device auth-mode.
B. Leave all edge ports in client auth-mode and configure device auth-mode in the AP role.
C. Configure all edge ports in client auth-mode.
D. Leave all edge ports in device auth-mode and configure client auth-mode in the AP role.

Correct Answer: C
Section:
Explanation:
For a company with AOS-CX switches and HPE Aruba Networking APs running AOS-10, where 802.1X authentication is required on all edge ports, you should configure all edge ports in client auth-mode. This mode ensures that each client connecting through the APs is authenticated individually, maintaining the security policy requirements for 802.1X authentication on all connections.

QUESTION 16
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.

Correct Answer: D
Section:
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.

QUESTION 17
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

Correct Answer: D
Section:
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.

QUESTION 18
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

Correct Answer: D
Section:
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.

QUESTION 19
Your company wants to implement Tunneled EAP (TEAP).
How can you set up HPE Aruba Networking ClearPass Policy Manager (CPPM) to enforce certificated-based 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.

Correct Answer: D
Section:
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.

QUESTION 20
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.

Correct Answer: B
Section:
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.

QUESTION 21
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.

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

QUESTION 22
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.

Correct Answer: A
Section:
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.

QUESTION 23
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)

Correct Answer: D
Section:
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.

QUESTION 24
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.

Correct Answer: A
Section:
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.

QUESTION 25
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.

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

QUESTION 26
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.

Correct Answer: C
Section:
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 27
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.

Correct Answer: A
Section:
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 28
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.

Correct Answer: D
Section:
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 29
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.

Correct Answer: C
Section:
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 30
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.

Correct Answer: A
Section:
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 31
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 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.

Correct Answer: D
Section:
Explanation:
802.1X 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 32
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.

Correct Answer: B
Section:
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 33
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

Correct Answer: C
Section:
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.

QUESTION 34
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.

Correct Answer: B
Section:
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.

QUESTION 35
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

Correct Answer: C
Section:
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.

QUESTION 36
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.

Correct Answer: C
Section:
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.

QUESTION 37
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

Correct Answer: B
Section:
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.

QUESTION 38
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

Correct Answer: A
Section:
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.

QUESTION 39
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. Use Syslog to integrate the gateways with HPE Aruba Networking ClearPass Policy Manager (CPPM) event processing.
B. Integrate HPE Aruba Networking ClearPass Device Insight (CPDI) with Central and schedule hourly reports.
C. Set up email notifications using HPE Aruba Networking Central's global alert settings.
D. Set up Webhooks that are attached to the HPE Aruba Networking Central Threat Dashboard.

Correct Answer: C
Section:
Explanation:
For a faster way to discover if a gateway starts detecting threats in traffic, admins should set up email notifications using HPE Aruba Networking Central's global alert settings. This setup ensures that the security team is promptly informed via email whenever the IDS/IPS on the gateways detects any threats, allowing for immediate investigation and response.
1. Email Notifications: By configuring email notifications, admins can receive real-time alerts directly to their inbox, reducing the time to discover and react to security incidents.
2. Global Alert Settings: HPE Aruba Networking Central's global alert settings allow for customization of alerts based on specific security events and thresholds, providing flexibility in monitoring and response.
3. Proactive Monitoring: This proactive approach ensures that the security team is always aware of potential threats without the need to constantly check the Security Dashboard manually.

QUESTION 40

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

Correct Answer: B
Section:
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.

QUESTION 41
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

Correct Answer: A
Section:
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.

QUESTION 42
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.

Correct Answer: A
Section:
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.

QUESTION 43
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.

Correct Answer: D
Section:
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.

QUESTION 44
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.

Correct Answer: B
Section:
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.

QUESTION 45
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.

Correct Answer: A
Section:
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 User-Agent 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.

QUESTION 46
Which statement describes Zero Trust Security?

A. Companies should focus on protecting their resources rather than on protecting the boundaries of their internal network.
B. Companies must apply the same access controls to all users, regardless of identity.
C. Companies that support remote workers cannot achieve zero trust security and must determine if the benefits outweigh the cost.
D. Companies can achieve zero trust security by strengthening their perimeter security to detect a wider range of threats.

Correct Answer: A
Section:
Explanation:
Zero Trust Security is a security model that operates on the principle that no entity, whether inside or outside the network, should be trusted by default. Instead, every access request is thoroughly verified before granting access to resources. This model emphasizes protecting resources rather than merely securing the network perimeter, acknowledging that threats can originate both inside and outside the network.
1. Resource Protection: Zero Trust focuses on securing individual resources, assuming that threats can bypass traditional perimeter defenses.
2. Verification: Every access request is authenticated and authorized regardless of the source, ensuring that only legitimate users can access sensitive resources.
3. Modern Security Approach: This model aligns with the evolving threat landscape where insider threats and advanced persistent threats are common.

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

Correct Answer: A
Section:
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.

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.

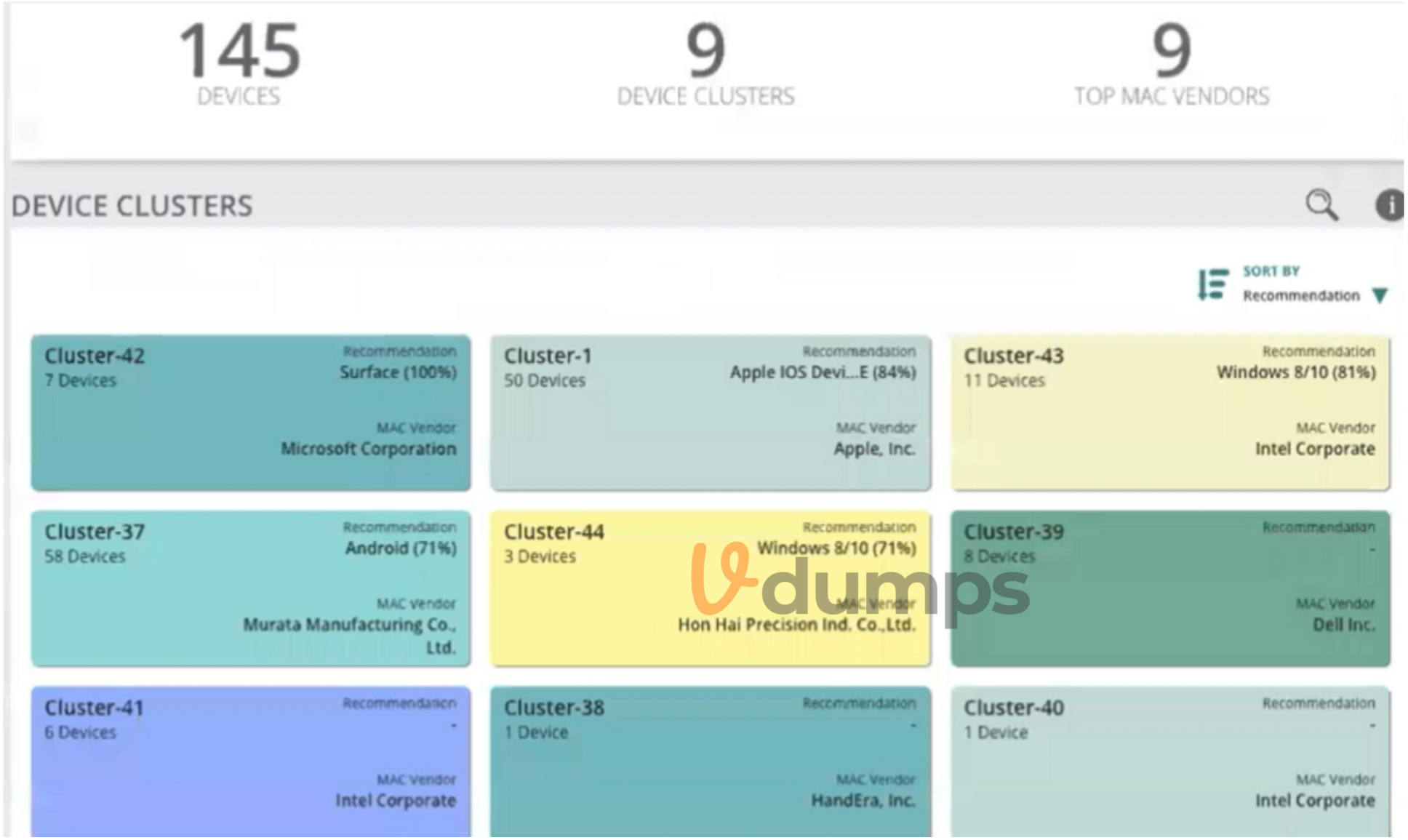
Correct Answer: B
Section:
Explanation:
To ensure that the correct profiles apply after client attributes are updated based on Syslog messages, you should tune the Change of Authorization (CoA) delay on the ClearPass servers to a value of 5 seconds or greater. This delay allows sufficient time for the attribute updates to be processed and for the reauthentication to occur correctly, ensuring that the updated profiles are accurately applied to the clients.
1. CoA Delay: Adjusting the CoA delay ensures that the system has enough time to update client attributes and reauthenticate them properly before applying new profiles.
2. Profile Accuracy: This delay helps in preventing premature reauthentication and ensures that the most recent attribute updates are considered when applying profiles.
3. System Synchronization: Ensures synchronization between the attribute update and the reauthentication process.

QUESTION 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.

Correct Answer: D
Section:
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.

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.

Correct Answer: A
Section:
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.

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.

Correct Answer: B
Section:
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.

QUESTION 52
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

Correct Answer: C
Section:
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.

QUESTION 53
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.

Correct Answer: C
Section:
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.

QUESTION 54
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.

Correct Answer: C
Section:
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.

QUESTION 55
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.

Correct Answer: A
Section:

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.