Vendor: HP

Exam Code: HPE7-A02

Exam Name: Aruba Certified Network Security Professional Exam

Version: DEMO

QUESTION 1
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.

QUESTION 2
A company lacks visibility into the many different types of user and IoT 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.

QUESTION 3
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.

QUESTION 4
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.

QUESTION 5
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.

QUESTION 6
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.

QUESTION 7
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.

Answer: C
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 8

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.

QUESTION 9
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.

QUESTION 10
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.

QUESTION 11
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.

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.

QUESTION 12
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.

QUESTION 13
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.

QUESTION 15
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.

Thank You for Trying Our Product

Passleader Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.passleader.com/all-products.html

10% Discount Coupon Code: **ASTR14**