HP.HPE6-A78.v2026-01-19.q107

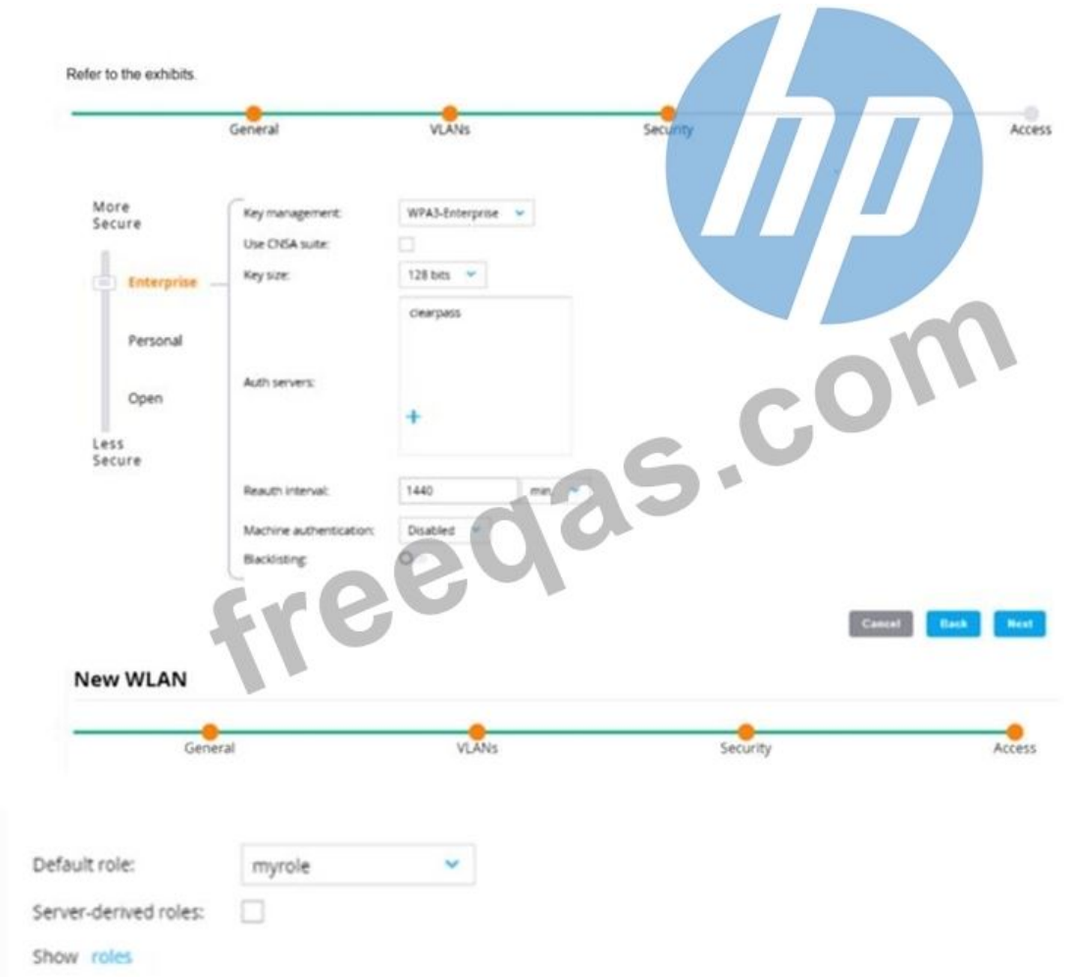
Exam Code:	HPE6-A78
Exam Name:	Aruba Certified Network Security Associate Exam
Certification Provider:	HP
Free Question Number:	107
Version:	v2026-01-19
# of views:	114
# of Questions views:	1070
https://www.freeqas.com/qa/HP/HPE6-A78/HP.HPE6-A78.v2026-01-19.q107.html	

NEW QUESTION: 1
Refer to the exhibit.

This Aruba Mobility Controller (MC) should authenticate managers who access the Web UI to ClearPass Policy Manager (CPPM) ClearPass admins have asked you to use RADIUS and explained that the MC should accept managers' roles in Aruba-Admin-Role VSAs Which setting should you change to follow Aruba best security practices?

A. Change the local user role to read-only
B. Clear the MSCHAP check box
C. Disable local authentication
D. Change the default role to "guest-provisioning"
Answer: (SHOW ANSWER)
For following Aruba best security practices, the setting you should change is to disable local authentication. When integrating with an external RADIUS server like ClearPass Policy Manager (CPPM) for authenticating administrative access to the Mobility Controller (MC), it is a best practice to rely on the external server rather than the local user database. This practice not only centralizes the management of user roles and access but also enhances security by leveraging CPPM's advanced authentication mechanisms.
:
Aruba Networks official best practice documentation, which recommends centralized authentication for administrative access.
Security standards and guidelines that promote the use of external RADIUS servers for authentication purposes.

NEW QUESTION: 2
Refer to the exhibit.



An admin has created a WLAN that uses the settings shown in the exhibits (and has not otherwise adjusted the settings in the AAA profile) A client connects to the WLAN Under which circumstances will a client receive the default role assignment?

A. The client has attempted 802 1X authentication, but the MC could not contact the authentication server

B. The client has attempted 802 1X authentication, but failed to maintain a reliable connection, leading to a timeout error

C. The client has passed 802 1X authentication, and the value in the Aruba-User-Role VSA matches a role on the MC

D. The client has passed 802 1X authentication and the authentication server did not send an Aruba-User-Role VSA

Answer: D (LEAVE A REPLY)

In the context of an Aruba Mobility Controller (MC) configuration, a client will receive the default role assignment if they have passed 802.1X authentication and the authentication server did not send an Aruba-User-Role Vendor Specific Attribute (VSA). The default role is assigned by the MC when a client successfully authenticates but the authentication server provides no specific role instruction. This behavior ensures that a client is not left without any role assignment, which could potentially lead to a lack of network access or access control. This default role assignment mechanism is part of Aruba's role-based access control, as documented in the ArubaOS user guide and best practices.

NEW QUESTION: 3

What is one difference between EAP-Tunneled Layer security (EAP-TLS) and Protected EAP (PEAP)?

A. EAP-TLS begins with the establishment of a TLS tunnel, but PEAP does not use a TLS tunnel as part of Its process

B. EAP-TLS requires the supplicant to authenticate with a certificate, hut PEAP allows the supplicant to use a username and password.

C. EAP-TLS creates a TLS tunnel for transmitting user credentials, while PEAP authenticates the server and supplicant during a TLS handshake.

D. EAP-TLS creates a TLS tunnel for transmitting user credentials securely while PEAP protects user credentials with TKIP encryption.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 4

Device A is contacting https://arubapedia.arubanetworks.com. The web server sends a certificate chain. What does the browser do as part of validating the web server certificate?

A. It makes sure that the key in the certificate matches the key that DeviceA uses for HTTPS.

B. It makes sure the certificate has a DNS SAN that matches arubapedia.arubanetworks.com

C. It makes sure that the public key in the certificate matches DeviceA's private HTTPS key.

D. It makes sure that the public key in the certificate matches a private key stored on DeviceA.

Answer: B (LEAVE A REPLY)
When a device like Device A contacts a secure website and receives a certificate chain from the server, the browser's primary task is to validate the web server's certificate to ensure it is trustworthy. Part of this validation includes checking that the certificate contains a DNS Subject Alternative Name (SAN) that matches the domain name of the website being accessed-in this case, arubapedia.arubanetworks.com. This ensures that the certificate was indeed issued to the entity operating the domain and helps prevent man-in-the-middle attacks where an invalid certificate could be presented by an attacker. The DNS SAN check is critical because it directly ties the digital certificate to the domain it secures, confirming the authenticity of the website to the user's browser.

NEW QUESTION: 5
What is one benefit of enabling Enhanced Secure mode on an ArubaOS-Switch?
A. Control Plane policing rate limits edge ports to mitigate DoS attacks on network servers.
B. A self-signed certificate is automatically added to the switch trusted platform module (TPM).
C. Insecure algorithms for protocol such as SSH are automatically disabled.
D. All interfaces have 802.1X authentication enabled on them by default.
Answer: C (LEAVE A REPLY)
In the context of ArubaOS-Switches, enabling Enhanced Secure mode has several benefits, one of which includes disabling insecure algorithms for protocols such as SSH. This is in line with security best practices, as older, less secure algorithms are known to be vulnerable to various types of cryptographic attacks. When Enhanced Secure mode is enabled, the switch automatically restricts the use of such algorithms, thereby enhancing the security of management access.

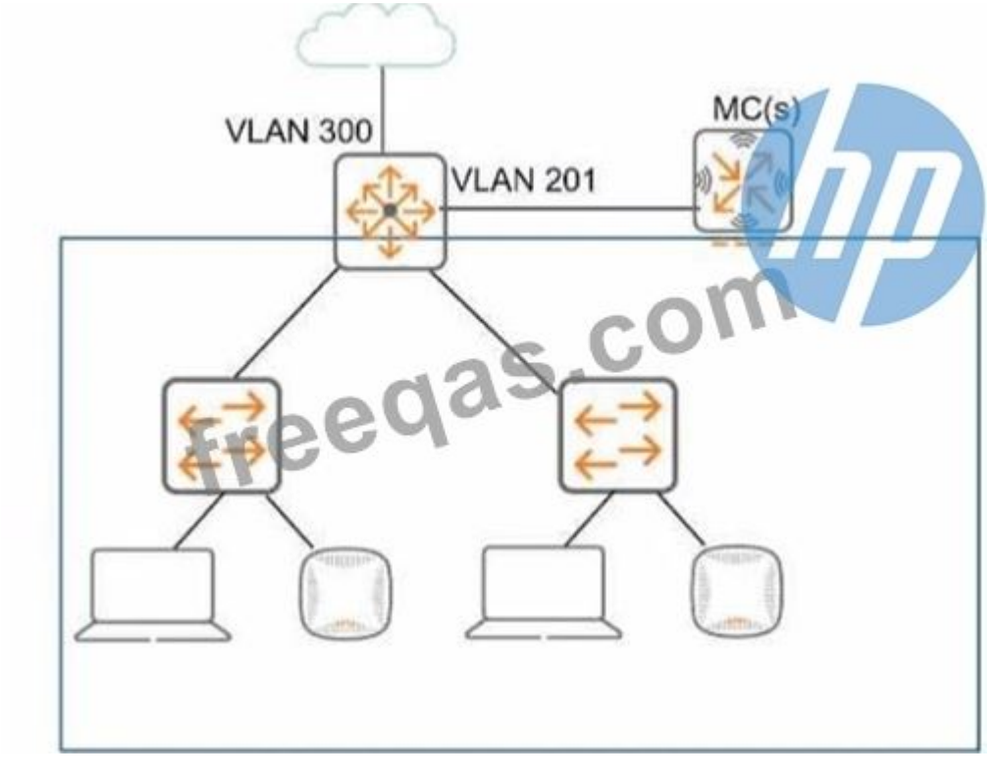
NEW QUESTION: 6
What is a use case for Transport Layer Security (TLS)?
A. to establish a framework for devices to determine when to trust other devices' certificates
B. to enable a client and a server to establish secure communications for another protocol
C. to enable two parties to asymmetrically encrypt and authenticate all data that passes be-tween them
D. to provide a secure alternative to certificate authentication that is easier to implement
Answer: B (LEAVE A REPLY)
The use case for Transport Layer Security (TLS) is to enable a client and a server to establish secure communications for another protocol. TLS is a cryptographic protocol designed to provide secure communication over a computer network. It is widely used for web browsers and other applications that require data to be securely exchanged over a network, such as file transfers, VPN connections, and voice-over-IP (VoIP). TLS operates between the transport layer and the application layer of the Internet Protocol Suite and is used to secure various other protocols like HTTP (resulting in HTTPS), SMTP, IMAP, and more. This protocol ensures privacy and data integrity between two communicating applications. Detailed information about TLS and its use

cases can be found in IETF RFC 5246, which outlines the specifications for TLS 1.2, and in subsequent RFCs that define TLS 1.3.

NEW QUESTION: 7
How can hackers implement a man-in-the-middle (MITM) attack against a wireless client?
A. The hacker uses a combination of software and hardware to jam the RF band and prevent the client from connecting to any wireless networks.
B. The hacker runs an NMap scan on the wireless client to find its MAC and IP address. The hacker then connects to another network and spoofs those addresses.
C. The hacker connects a device to the same wireless network as the client and responds to the client's ARP requests with the hacker device's MAC address.
D. The hacker uses spear-phishing to probe for the IP addresses that the client is attempting to reach. The hacker device then spoofs those IP addresses.
Answer: (SHOW ANSWER)
A common method for hackers to perform a man-in-the-middle (MITM) attack on a wireless network is by ARP poisoning. The attacker connects to the same network as the victim and sends false ARP messages over the network. This causes the victim's device to send traffic to the attacker's machine instead of the legitimate destination, allowing the attacker to intercept the traffic.

NEW QUESTION: 8
Which is a correct description of a stage in the Lockheed Martin kill chain?
A. In the exploitation and installation phases, malware creates a backdoor into the infected system for the hacker.
B. In the reconnaissance stage, the hacker assesses the impact of the attack and how much information was exfilltrated.
C. In the delivery stage, malware collects valuable data and delivers or exfilltrated it to the hacker.
D. In the weaponization stage, which occurs after malware has been delivered to a system, the malware executes Its function.
Answer: A (LEAVE A REPLY)
The Lockheed Martin Cyber Kill Chain model describes the stages of a cyber attack. In the exploitation phase, the attacker uses vulnerabilities to gain access to the system. Following this, in the installation phase, the attacker installs a backdoor or other malicious software to ensure persistent access to the compromised system. This backdoor can then be used to control the system, steal data, or execute additional attacks.
References:
Lockheed Martin Cyber Kill Chain framework.

NEW QUESTION: 9
Refer to the exhibit, which shows the current network topology.



You are deploying a new wireless solution with an Aruba Mobility Master (MM). Aruba Mobility Controllers (MCs). and campus APs (CAPs). The solution will Include a WLAN that uses Tunnel for the forwarding mode and Implements WPA3-Enterprise security What is a guideline for setting up the vlan for wireless devices connected to the WLAN?

A. Use wireless user roles to assign the devices to different VLANs in the 100-150 range

B. Use wireless user roles to assign the devices to a range of new vlan IDs.

C. Assign the WLAN to a named VLAN which specified 100-150 as the range of IDs.

D. Assign the WLAN to a single new VLAN which is dedicated to wireless users

Answer: (SHOW ANSWER)

NEW QUESTION: 10

A client is connected to a Mobility Controller (MC). These firewall rules apply to this client's role:

ipv4 any any svc-dhcp permit

ipv4 user 10.5.5.20 svc-dns permit

ipv4 user 10.1.5.0 255.255.255.0 https permit

ipv4 user 10.1.0.0 255.255.0.0 https deny_opt

ipv4 user any any permit

What correctly describes how the controller treats HTTPS packets to these two IP addresses, both of which are on the other side of the firewall:

10.1.20.1

10.5.5.20

A. Both packets are denied.

B. The first packet is permitted, and the second is denied.

C. Both packets are permitted.

D. The first packet is denied, and the second is permitted.

Answer: (SHOW ANSWER)

In an HPE Aruba Networking AOS-8 Mobility Controller (MC), firewall rules are applied based on the user role assigned to a client. The rules are evaluated in order, and the first matching rule determines the action (permit or deny) for the packet. The client's role has the following firewall rules:

ipv4 any any svc-dhcp permit: Permits DHCP traffic (UDP ports 67 and 68) from any source to any destination.

ipv4 user 10.5.5.20 svc-dns permit: Permits DNS traffic (UDP port 53) from the user to the IP address 10.5.5.20.

ipv4 user 10.1.5.0 255.255.255.0 https permit: Permits HTTPS traffic (TCP port 443) from the user to the subnet 10.1.5.0/24.

ipv4 user 10.1.0.0 255.255.0.0 https deny_opt: Denies HTTPS traffic from the user to the subnet 10.1.0.0/16, with the deny_opt action (which typically means deny with an optimized action, such as dropping the packet without logging).

ipv4 user any any permit: Permits all other traffic from the user to any destination.

The question asks how the MC treats HTTPS packets (TCP port 443) to two IP addresses: 10.1.20.1 and 10.5.5.20.

HTTPS packet to 10.1.20.1:

Rule 1: Does not match (traffic is HTTPS, not DHCP).

Rule 2: Does not match (destination is 10.1.20.1, not 10.5.5.20; traffic is HTTPS, not DNS).

Rule 3: Does not match (destination 10.1.20.1 is not in the subnet 10.1.5.0/24).

Rule 4: Matches (destination 10.1.20.1 is in the subnet 10.1.0.0/16, and traffic is HTTPS). The action is deny_opt, so the packet is denied.

HTTPS packet to 10.5.5.20:

Rule 1: Does not match (traffic is HTTPS, not DHCP).

Rule 2: Does not match (traffic is HTTPS, not DNS).

Rule 3: Does not match (destination 10.5.5.20 is not in the subnet 10.1.5.0/24).

Rule 4: Does not match (destination 10.5.5.20 is not in the subnet 10.1.0.0/16).

Rule 5: Matches (catches all other traffic). The action is permit, so the packet is permitted.

Therefore, the HTTPS packet to 10.1.20.1 is denied, and the HTTPS packet to 10.5.5.20 is permitted.

Option A, "Both packets are denied," is incorrect because the packet to 10.5.5.20 is permitted.

Option B, "The first packet is permitted, and the second is denied," is incorrect because the packet to 10.1.20.1 (first) is denied, and the packet to 10.5.5.20 (second) is permitted.

Option C, "Both packets are permitted," is incorrect because the packet to 10.1.20.1 is denied.

Option D, "The first packet is denied, and the second is permitted," is correct based on the rule evaluation.

The HPE Aruba Networking AOS-8 8.11 User Guide states:

"Firewall policies on the Mobility Controller are evaluated in order, and the first matching rule determines the action for the packet. For example, a rule such as ipv4 user 10.1.0.0 255.255.0.0 https deny_opt will deny HTTPS traffic to the specified subnet, while a subsequent rule like ipv4

user any any permit will permit all other traffic that does not match earlier rules. The 'user' keyword in the rule refers to the client's IP address, and the rules are applied to traffic initiated by the client." (Page 325, Firewall Policies Section) Additionally, the guide notes:
"The deny_opt action in a firewall rule drops the packet without logging, optimizing performance for high-volume traffic. Rules are processed sequentially, and only the first matching rule is applied." (Page 326, Firewall Actions Section)
:
HPE Aruba Networking AOS-8 8.11 User Guide, Firewall Policies Section, Page 325.
HPE Aruba Networking AOS-8 8.11 User Guide, Firewall Actions Section, Page 326.

NEW QUESTION: 11
You have a network with ArubaOS-Switches for which Aruba ClearPass Policy Manager (CPPM) is acting as a TACACS+ server to authenticate managers. CPPM assigns the admins a TACACS + privilege level, either manager or operator. You are now adding ArubaOS-CX switches to the network. ClearPass admins want to use the same CPPM service and policies to authenticate managers on the new switches.
What should you explain?
A. This approach cannot work because the ArubaOS-CX switches do not accept standard TACACS+ privilege levels.
B. This approach cannot work because the ArubaOS-CX switches do not support TACACS+.
C. This approach will work, but will need to be adjusted later if you want to assign managers to the default auditors group.
D. This approach will work to assign admins to the default "administrators" group, but not to the default
"operators" group.
Answer: D (LEAVE A REPLY)
With ArubaOS-CX switches, the use of ClearPass Policy Manager (CPPM) as a TACACS+ server for authentication is supported. The privilege levels assigned by CPPM will translate onto the switches, where the "manager" privilege level typically maps to administrative capabilities and the "operator" privilege level maps to more limited capabilities. ArubaOS-CX does support standard TACACS+ privilege levels, so administrators can be assigned appropriately. If the ClearPass policies are correctly configured, they will work for both ArubaOS-Switches and ArubaOS-CX switches. The distinction between the "administrators" and "operators" groups is inherent in the ArubaOS-CX role-based access control, and these default groups need to be appropriately mapped to the TACACS+ privilege levels assigned by CPPM.

NEW QUESTION: 12
A user is having trouble connecting to an AP managed by a standalone Mobility Controller (MC). What can you do to get detailed logs and debugs for that user's client?
A. In the MC CLI, set up a control plane packet capture and filter for the client's IP address.
B. In the MC CLI, set up a data plane packet capture and filter for the client's MAC address.

C. In the MC UI's Traffic Analytics dashboard, look for the client's IP address.
D. In the MC UI's Diagnostics > Logs pages, add a "user-debug" log setting for the client's MAC address.
Answer: D (LEAVE A REPLY)
When troubleshooting connectivity issues for a user connecting to an AP managed by a standalone Mobility Controller (MC) in an AOS-8 architecture, detailed logs and debugs specific to the user's client are essential. The MC provides several tools for capturing logs and debugging information, including packet captures and user-specific debug logs.
Option D, "In the MC UI's Diagnostics > Logs pages, add a 'user-debug' log setting for the client's MAC address," is correct. The "user-debug" feature in the MC allows administrators to enable detailed debugging for a specific client by specifying the client's MAC address. This generates logs related to the client's authentication, association, role assignment, and other activities, which are critical for troubleshooting connectivity issues. The Diagnostics > Logs pages in the MC UI provide a user-friendly way to configure this setting and view the resulting logs.
Option A, "In the MC CLI, set up a control plane packet capture and filter for the client's IP address," is incorrect because control plane packet captures are used to capture management traffic (e.g., between the MC and APs or other controllers), not user traffic. Additionally, the client may not yet have an IP address if connectivity is failing, making an IP-based filter less effective.
Option B, "In the MC CLI, set up a data plane packet capture and filter for the client's MAC address," is a valid troubleshooting method but is not the best choice for getting detailed logs. Data plane packet captures are useful for analyzing user traffic (e.g., to see if packets are being dropped), but they do not provide the same level of detailed logging as the "user-debug" feature, which includes authentication and association events.
Option C, "In the MC UI's Traffic Analytics dashboard, look for the client's IP address," is incorrect because the Traffic Analytics dashboard is used for monitoring application usage and traffic patterns, not for detailed troubleshooting of a specific client's connectivity issues. Additionally, if the client cannot connect, it may not have an IP address or generate traffic visible in the dashboard.
The HPE Aruba Networking AOS-8 8.11 User Guide states:
"To troubleshoot issues for a specific wireless client, you can enable user-specific debugging using the 'user-debug' feature. In the Mobility Controller UI, navigate to Diagnostics > Logs, and add a 'user-debug' log setting for the client's MAC address. This will generate detailed logs for the client, including authentication, association, and role assignment events, which can be viewed in the Logs page. For example, to enable user-debug for a client with MAC address 00:11:22:33:44:55, add the setting 'user-debug 00:11:22:33:44:55'." (Page 512, Troubleshooting Wireless Clients Section) Additionally, the guide notes:
"While packet captures (control plane or data plane) can be useful for analyzing traffic, the 'user-debug' feature provides more detailed logs for troubleshooting client-specific issues, such as failed authentication or association problems." (Page 513, Debugging Tools Section)
:

HPE Aruba Networking AOS-8 8.11 User Guide, Troubleshooting Wireless Clients Section, Page 512.
HPE Aruba Networking AOS-8 8.11 User Guide, Debugging Tools Section, Page 513.

NEW QUESTION: 13
You have deployed a new HPE Aruba Networking Mobility Controller (MC) and campus APs (CAPs). One of the WLANs enforces 802.1X authentication to HPE Aruba Networking ClearPass Policy Manager (CPPM). When you test connecting the client to the WLAN, the test fails. You check ClearPass Access Tracker and cannot find a record of the authentication attempt. You ping from the MC to CPPM, and the ping is successful.
What is a good next step for troubleshooting?
A. Renew CPPM's RADIUS/EAP certificate.
B. Check connectivity between CPPM and a backend directory server.
C. Check CPPM Event Viewer.
D. Reset the user credentials.
Answer: (SHOW ANSWER)
In this scenario, a new HPE Aruba Networking Mobility Controller (MC) and campus APs (CAPs) are deployed, with a WLAN configured for 802.1X authentication using HPE Aruba Networking ClearPass Policy Manager (CPPM) as the RADIUS server. A client test fails, and no record of the authentication attempt appears in ClearPass Access Tracker. However, a ping from the MC to CPPM is successful, confirming basic network connectivity between the MC and CPPM.
The absence of a record in Access Tracker indicates that CPPM did not receive the RADIUS authentication request from the MC, or the request was rejected at a low level before being logged in Access Tracker. Access Tracker typically logs all RADIUS authentication attempts (successful or failed), so the lack of a record suggests a configuration or connectivity issue at the RADIUS level.
Option C, "Check CPPM Event Viewer," is correct. The CPPM Event Viewer logs system-level events, including RADIUS-related errors that might not appear in Access Tracker. For example, if the MC's IP address is not configured as a Network Access Device (NAD) in CPPM, or if the shared secret between the MC and CPPM does not match, CPPM may reject the RADIUS request before it reaches Access Tracker. The Event Viewer will log such errors (e.g., "RADIUS authentication attempt from unknown NAD"), providing insight into why the request was not processed.
Option A, "Renew CPPM's RADIUS/EAP certificate," is incorrect because the issue is that CPPM did not receive or process the authentication request (no record in Access Tracker). If there were a certificate issue (e.g., an expired or untrusted certificate), the request would still reach CPPM, and Access Tracker would log a failure with a certificate-related error.
Option B, "Check connectivity between CPPM and a backend directory server," is incorrect because the issue occurs before CPPM processes the authentication request. If CPPM cannot contact a backend directory server (e.g., Active Directory), the authentication attempt would still be logged in Access Tracker with a failure reason related to the directory server.

Option D, "Reset the user credentials," is incorrect because the issue is not related to the user's credentials. The authentication request never reached CPPM, so the credentials were not evaluated.
The HPE Aruba Networking ClearPass Policy Manager 6.11 User Guide states:
"If an authentication attempt does not appear in Access Tracker, it indicates that the RADIUS request was not received by ClearPass or was rejected at a low level before being logged. The Event Viewer (Monitoring > Event Viewer) should be checked for system-level errors, such as 'RADIUS authentication attempt from unknown NAD' or shared secret mismatches. For example, if the Network Access Device (NAD) IP address of the Mobility Controller is not configured in ClearPass, or if the shared secret does not match, the request will be dropped, and an error will be logged in the Event Viewer." (Page 301, Troubleshooting RADIUS Issues Section)
Additionally, the HPE Aruba Networking AOS-8 8.11 User Guide notes:
"When troubleshooting 802.1X authentication issues, verify that the Mobility Controller can communicate with the RADIUS server. If a ping is successful but no authentication records appear in the RADIUS server's logs (e.g., ClearPass Access Tracker), check the RADIUS server's system logs (e.g., ClearPass Event Viewer) for errors related to NAD configuration or shared secret mismatches." (Page 498, Troubleshooting 802.1X Authentication Section)
:
HPE Aruba Networking ClearPass Policy Manager 6.11 User Guide, Troubleshooting RADIUS Issues Section, Page 301.
HPE Aruba Networking AOS-8 8.11 User Guide, Troubleshooting 802.1X Authentication Section, Page 498.

NEW QUESTION: 14
What distinguishes a Distributed Denial of Service (DDoS) attack from a traditional Denial or service attack (DoS)?
A. A DDoS attack originates from external devices, while a DoS attack originates from internal devices
B. A DDoS attack is launched from multiple devices, while a DoS attack is launched from a single device
C. A DoS attack targets one server, a DDoS attack targets all the clients that use a server
D. A DDoS attack targets multiple devices, while a DoS Is designed to Incapacitate only one device
Answer: B (LEAVE A REPLY)
The main distinction between a Distributed Denial of Service (DDoS) attack and a traditional Denial of Service (DoS) attack is that a DDoS attack is launched from multiple devices, whereas a DoS attack originates from a single device. This distinction is critical because the distributed nature of a DDoS attack makes it more difficult to mitigate. Multiple attacking sources can generate a higher volume of malicious traffic, overwhelming the target more effectively than a single source, as seen in a DoS attack. DDoS attacks exploit a variety of devices across the

internet, often coordinated using botnets, to flood targets with excessive requests, leading to service degradation or complete service denial.
:
Cybersecurity texts and resources that differentiate between types of denial of service attacks.
Technical documentation and analysis of DDoS tactics, which illustrate how botnets and other distributed systems are employed to execute attacks.

NEW QUESTION: 15
What is symmetric encryption?
A. It any form of encryption mat ensures that thee ciphertext Is the same length as the plaintext.
B. It simultaneously creates ciphertext and a same-size MAC.
C. It uses a Key that is double the size of the message which it encrypts.
D. It uses the same key to encrypt plaintext as to decrypt ciphertext.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 16
You have been authorized to use containment to respond to rogue APs detected by ArubaOS Wireless Intrusion Prevention (WIP). What is a consideration for using tarpit containment versus traditional wireless containment?
A. Rather than function wirelessly, tarpit containment sends ARP frames over the wired network to poison rogue APs ARP tables and prevent them from transmitting on the wired network.
B. Rather than target all clients connected to rogue APs, tarpit containment targets only authorized clients that are connected to a rogue AP, reducing the chance of negative effects on neighbors.
C. Tarpit containment does not require an RF Protect license to function, while traditional wireless containment does.
D. Tarpit containment forms associations with clients to enable more effective containment with fewer disassociation frames than traditional wireless containment.
Answer: D (LEAVE A REPLY)
Tarpit containment is a method used in ArubaOS Wireless Intrusion Prevention (WIP) to contain rogue APs.
It differs from traditional wireless containment in several ways, particularly in how it interacts with clients and manages network resources.
Tarpit containment works by spoofing frames from an AP to confuse a client about its association. It forces the client to associate with a fake channel or BSSID, which is more efficient than rogue containment via repeated de-authorization requests. This method is designed to be less disruptive and more resource-efficient1.
Here's why the other options are not correct:
Option A is incorrect because tarpit containment does not involve sending ARP frames over the wired network. It operates wirelessly by creating a fake channel or BSSID.

Option B is incorrect because tarpit containment does not selectively target authorized clients; it affects all clients connected to the rogue AP.
Option C is incorrect because tarpit containment does require an RF Protect license to function2.
Therefore, Option D is the correct answer. Tarpit containment is more effective at keeping clients off the network with fewer disassociation frames than traditional wireless containment. It achieves this by forming associations with clients, which leads to a more efficient use of airtime and reduces the chance of negative effects on legitimate network users12.

NEW QUESTION: 17
What is a benefit of Opportunistic Wireless Encryption (OWE)?
A. It provides protection for wireless clients against both honeypot APs and man-in-the-middle (MUM) attacks
B. It offers more control over who can connect to the wireless network when compared with WPA2-Personal
C. It allows both WPA2-capabie and WPA3-capable clients to authenticate to the same WPA-Personal WLAN
D. It allows anyone lo connect, but provides better protection against eavesdropping than a traditional open network
Answer: D (LEAVE A REPLY)

NEW QUESTION: 18
What is one practice that can help you to maintain a digital chain or custody In your network?
A. Enable packet capturing on Instant AP or Moodily Controller (MC) datepath on an ongoing basis
B. Enable packet capturing on Instant AP or Mobility Controller (MC) control path on an ongoing basis.
C. Ensure that all network infrastructure devices receive a valid clock using authenticated NTP
D. Ensure that all network Infrastructure devices use RADIUS rather than TACACS+ to authenticate managers
Answer: (SHOW ANSWER)
To maintain a digital chain of custody in a network, a crucial practice is to ensure that all network infrastructure devices receive a valid clock using authenticated Network Time Protocol (NTP).

Accurate and synchronized time stamps are essential for creating reliable and legally defensible logs. Authenticated NTP ensures that the time being set on devices is accurate and that the time source is verified, which is necessary for correlating logs from different devices and for forensic analysis.
References:
Digital forensics and network security protocols that underscore the importance of accurate timekeeping for maintaining a digital chain of custody.
NTP configuration guidelines for network devices, emphasizing the use of authentication to prevent tampering with clock settings.

NEW QUESTION: 19
What is one of the roles of the network access server (NAS) in the AAA framewonx?
A. It enforces access to network services and sends accounting information to the AAA server
B. It authenticates legitimate users and uses policies to determine which resources each user is allowed to access.
C. It determines which resources authenticated users are allowed to access and monitors each users session
D. It negotiates with each user's device to determine which EAP method is used for authentication
Answer: B (LEAVE A REPLY)

NEW QUESTION: 20
From which solution can ClearPass Policy Manager (CPPM) receive detailed information about client device type OS and status?
A. ClearPass Access Tracker
B. ClearPass Guest
C. ClearPass OnGuard
D. ClearPass Onboard
Answer: C (LEAVE A REPLY)

NEW QUESTION: 21
You need to implement a WPA3-Enterprise network that can also support WPA2-Enterprise clients. What is a valid configuration for the WPA3-Enterprise WLAN?
A. CNSA mode disabled with 256-bit keys
B. CNSA mode disabled with 128-bit keys
C. CNSA mode enabled with 256-bit keys
D. CNSA mode enabled with 128-bit keys
Answer: A (LEAVE A REPLY)
In an Aruba network, when setting up a WPA3-Enterprise network that also supports WPA2-Enterprise clients, you would typically configure the network to operate in a transitional mode that supports both protocols. CNSA (Commercial National Security Algorithm) mode is intended for

networks that require higher security standards as specified by the US National Security Agency (NSA). However, for compatibility with WPA2 clients, which do not support CNSA requirements, you would disable CNSA mode. WPA3 can use 256-bit encryption keys, which offer a higher level of security than the 128-bit keys used in WPA2.

NEW QUESTION: 22
Which scenario requires the Aruba Mobility Controller to use a Server Certificate?
A. Obtain downloadable user roles (DURs) from ClearPass.
B. Synchronize its clock with an NTP server that requires authentication.
C. Use RadSec for enforcing 802.1X authentication to ClearPass.
D. Use RADIUS for enforcing 802.1X authentication to ClearPass.
Answer: (SHOW ANSWER)
A Server Certificate is required by Aruba Mobility Controller when using RadSec to secure RADIUS communication. RadSec provides a secure transport for RADIUS traffic through SSL/TLS which requires the use of a Server Certificate to establish the secure tunnel. In the other scenarios listed, a Server Certificate is not explicitly required for the operations mentioned.

NEW QUESTION: 23

Refer to the exhibit.

A company has an Aruba Instant AP cluster. A Windows 10 client is attempting to connect a WLAN that enforces WPA3-Enterprise with authentication to ClearPass Policy Manager (CPPM). CPPM is configured to require EAP-TLS. The client authentication fails. In the record for this client's authentication attempt on CPPM, you see this alert.
What is one thing that you check to resolve this issue?
A. whether the client has a third-party 802.1 X supplicant, as Windows 10 does not support EAP-TLS
B. whether the client has a valid certificate installed on it to let it support EAP-TLS
C. whether EAP-TLS is enabled in the SSID Profile settings for the WLAN on the IAP cluster
D. whether EAP-TLS is enabled in the AAA Profile settings for the WLAN on the IAP cluster
Answer: B (LEAVE A REPLY)

In the context of WPA3-Enterprise with EAP-TLS authentication, the error message "Client doesn't support configured EAP methods" suggests that the client is not able to complete the EAP-TLS authentication process. EAP-TLS requires that both the server (in this case, CPPM) and the client have a valid certificate for mutual authentication. Windows 10 does support EAP-TLS natively, so options A, C, and D can be ruled out.
The most likely reason for the authentication failure is that the client device does not have the correct client certificate installed, which is required to establish a TLS session with the server. Therefore, ensuring that the client has a valid certificate installed that matches the server's requirements is the correct step to resolve this issue.

NEW QUESTION: 24
Refer to the exhibit.

Device A is establishing an HTTPS session with the Arubapedia web sue using Chrome. The Arubapedia web server sends the certificate shown in the exhibit What does the browser do as part of vacating the web server certificate?
A. It uses the private key in the Arubapedia web site's certificate to check that certificate's signature

B. It uses the private key in the DigiCert SHA2 Secure Server CA to check the certificate's signature.
C. It uses the public key in the DigCert root CA certificate to check the certificate signature
D. It uses the public key in the DigCen SHA2 Secure Server CA certificate to check the certificate's signature.
Answer: (SHOW ANSWER)

NEW QUESTION: 25
What is a correct use case for using the specified certificate file format?
A. using a PKCS7 file to install a certificate plus and its private key on a device
B. using a PKCS12 file to install a certificate plus its private key on a device
C. using a PEM file to install a binary encoded certificate on a device
D. using a PKCS7 file to install a binary encoded private key on a device
Answer: B (LEAVE A REPLY)
The correct use case for using the specified certificate file format is option B, using a PKCS12 file to install a certificate along with its private key on a device. PKCS12 is a binary format for storing a certificate chain and private key in a single encrypted file. PEM files are Base64 encoded certificate files and are typically used for storing certificates, not private keys, and PKCS7 is used for certificate chains without the private key.
These answers are based on general networking and security practices, specifically within the context of Aruba network device configurations. If you have questions specific to Oracle Database 12c SQL, please provide the relevant details or ask separate questions related to that topic.

NEW QUESTION: 26
Which correctly describes a way to deploy certificates to end-user devices?
A. ClearPass Onboard can help to deploy certificates to end-user devices, whether or not they are members of a Windows domain
B. ClearPass Device Insight can automatically discover end-user devices and deploy the proper certificates to them
C. ClearPass OnGuard can help to deploy certificates to end-user devices, whether or not they are members of a Windows domain
D. in a Windows domain, domain group policy objects (GPOs) can automatically install computer, but not user certificates
Answer: A (LEAVE A REPLY)

NEW QUESTION: 27
You need to set up Aruba network infrastructure devices for management with SNMP. The SNMP server has this SNMPv3 user configured on it: username: airwave auth algorithm: sha auth key: fyluqp18@S!9a priv algorithm: aes priv key: 761oxaiaoeu19& What correctly describes the setup on the infrastructure device?

A. You must configure a user with the same name and keys, but can choose algorithms that meet the device's needs.
B. You must configure the "airwave" server as an authorized user. Then, configure a separate user for this device with its own keys.
C. You must configure a user with the same name and algorithms, but the keys should be unique to this device.
D. You must configure a user with exactly the same name, algorithms, and keys.
Answer: D (LEAVE A REPLY)
In SNMPv3, security is paramount and each SNMP entity (client or agent) needs to have a user with a security name (username) and optionally, a security level which determines whether authentication and encryption are used. When configuring SNMPv3 users on network infrastructure devices, it is essential to match the username, authentication (auth) algorithm, authentication key (auth key), privacy (priv) algorithm, and privacy key (priv key) exactly as they are configured on the SNMP server to ensure successful communication.
This is because the SNMPv3 security model relies on a combination of a username and a pair of keys (authentication and privacy keys) to uniquely identify and secure communication between the agent and the manager. The keys are used to verify the integrity (auth key) and confidentiality (priv key) of the messages.
Using the same algorithms ensures that the messages can be properly encrypted and decrypted on both ends.

NEW QUESTION: 28
What is one way that Control Plane Security (CPSec) enhances security for the network?
A. It protects management traffic between APs and Mobility Controllers (MCs) from eavesdropping.
B. It prevents Denial of Service (DoS) attacks against Mobility Controllers' (MCs') control plane.
C. It protects wireless clients' traffic, tunneled between APs and Mobility Controllers, from eavesdropping.
D. It prevents access from unauthorized IP addresses to critical services, such as SSH, on Mobility Controllers (MCs).
Answer: A (LEAVE A REPLY)
Control Plane Security (CPSec) is a feature in HPE Aruba Networking's AOS-8 architecture that secures the communication between Access Points (APs) and Mobility Controllers (MCs). The control plane includes management traffic, such as AP registration, configuration updates, and heartbeat messages, which are critical for the operation of the wireless network.
Option A, "It protects management traffic between APs and Mobility Controllers (MCs) from eavesdropping," is correct. CPSec uses certificate-based authentication and encryption (IPSec tunnels) to secure the control plane communication between APs and MCs. This ensures that management traffic, which includes sensitive information like configuration data and AP status, is encrypted and protected from eavesdropping by unauthorized parties on the network.

Option B, "It prevents Denial of Service (DoS) attacks against Mobility Controllers' (MCs') control plane," is incorrect. While CPSec enhances security by authenticating APs and encrypting traffic, it is not specifically designed to prevent DoS attacks. DoS attacks against the control plane are mitigated by other features, such as rate limiting or firewall policies on the MC.
Option C, "It protects wireless clients' traffic, tunneled between APs and Mobility Controllers, from eavesdropping," is incorrect. CPSec protects the control plane (management traffic), not the data plane (client traffic). Client traffic in a tunneled architecture (e.g., GRE tunnels) is protected by the client's wireless encryption (e.g., WPA3), not CPSec.
Option D, "It prevents access from unauthorized IP addresses to critical services, such as SSH, on Mobility Controllers (MCs)," is incorrect. CPSec does not control access to services like SSH on the MC. Access to such services is managed by other features, such as access control lists (ACLs) or management authentication settings on the MC.
The HPE Aruba Networking AOS-8 8.11 User Guide states:
"Control Plane Security (CPSec) enhances network security by protecting the management traffic between Access Points (APs) and Mobility Controllers (MCs). When CPSec is enabled, the control plane communication is secured using certificate-based authentication and IPSec encryption, preventing eavesdropping and ensuring that only authorized APs can communicate with the MC. This protects sensitive management data, such as AP configuration and status updates, from being intercepted." (Page 392, CPSec Overview Section) Additionally, the HPE Aruba Networking CPSec Deployment Guide notes:
"CPSec secures the control plane by encrypting management traffic between APs and MCs, ensuring that attackers cannot eavesdrop on or tamper with this communication. It does not protect client data traffic, which is secured by wireless encryption protocols like WPA3." (Page 8, CPSec Benefits Section)
:
HPE Aruba Networking AOS-8 8.11 User Guide, CPSec Overview Section, Page 392.
HPE Aruba Networking CPSec Deployment Guide, CPSec Benefits Section, Page 8.

NEW QUESTION: 29
You are managing an Aruba Mobility Controller (MC). What is a reason for adding a "Log Settings" definition in the ArubaOS Diagnostics > System > Log Settings page?
A. Configuring a filter that you can apply to a defined Syslog server in order to filter events by subcategory
B. Configuring the log facility and log format that the MC will use for forwarding logs to all Syslog servers
C. Configuring the Syslog server settings for the server to which the MC forwards logs for a particular category and level
D. Configuring the MC to generate logs for a particular event category and level, but only for a specific user or AP.
Answer: (SHOW ANSWER)

NEW QUESTION: 30
A company has an ArubaOS controller-based solution with a WPA3-Enterprise WLAN. which authenticates wireless clients to Aruba ClearPass Policy Manager (CPPM). The company has decided to use digital certificates for authentication A user's Windows domain computer has had certificates installed on it However, the Networks and Connections window shows that authentication has tailed for the user. The Mobility Controllers (MC's) RADIUS events show that it is receiving Access-Rejects for the authentication attempt.
What is one place that you can you look for deeper insight into why this authentication attempt is failing?
A. the Alerts tab in the authentication record in CPPM Access Tracker
B. the reports generated by Aruba ClearPass Insight
C. the packets captured on the MC control plane destined to UDP 1812
D. the RADIUS events within the CPPM Event Viewer
Answer: A (LEAVE A REPLY)

NEW QUESTION: 31
You have deployed a new Aruba Mobility Controller (MC) and campus APs (CAPs). One of the WLANs enforces 802.IX authentication lo Aruba ClearPass Policy Manager {CPPM) When you test connecting the client to the WLAN. the test falls You check Aruba ClearPass Access Tracker and cannot find a record of the authentication attempt You ping from the MC to CPPM. and the ping is successful.
What is a good next step for troubleshooting?
A. Renew CPPM's RADIUS/EAP certificate
B. Reset the user credentials
C. Check CPPM Event viewer.
D. Check connectivity between CPPM and a backend directory server
Answer: C (LEAVE A REPLY)
When dealing with a failed 802.1X authentication attempt to a WLAN enforced by Aruba ClearPass Policy Manager (CPPM) where no record of the attempt is seen in ClearPass Access Tracker, a good next troubleshooting step is to check the CPPM Event Viewer. Since you are able to successfully ping from the Mobility Controller to CPPM, this indicates that there is network connectivity between these two devices.
The lack of a record in Access Tracker suggests that the issue may not be with the RADIUS/EAP certificate or user credentials, but possibly with the ClearPass service itself or its reception of authentication requests.
The Event Viewer can provide detailed logs that might reveal internal errors or misconfigurations within CPPM that could prevent it from processing authentication attempts properly.

NEW QUESTION: 32
What is a consideration for implementing wireless containment in response to unauthorized devices discovered by ArubaOS Wireless Intrusion Detection (WIP)?
A. It is best practice to implement automatic containment of unauthorized devices to eliminate the need to locate and remove them.
B. Wireless containment only works against unauthorized wireless devices that connect to your corporate LAN, so it does not offer protection against Interfering APs.
C. Your company should consider legal implications before you enable automatic containment or implement manual containment.
D. Because wireless containment has a lower risk of targeting legitimate neighbors than wired containment, it is recommended in most use cases.
Answer: (SHOW ANSWER)
When implementing wireless containment as a response to unauthorized devices, a company should consider the legal implications. Wireless containment might affect devices that are not part of the company's network and could be considered as a form of interference. This could have legal consequences, and therefore, such actions should be carefully reviewed and ideally should be performed in a targeted and controlled manner, reducing the risk of legal issues.

NEW QUESTION: 33
What is a benefit of Opportunistic Wireless Encryption (OWE)?
A. It allows both WPA2-capable and WPA3-capable clients to authenticate to the same WPA-Personal WLAN.
B. It offers more control over who can connect to the wireless network when compared with WPA2-Personal.
C. It allows anyone to connect, but provides better protection against eavesdropping than a traditional open network.
D. It provides protection for wireless clients against both honeypot APs and man-in-the-middle (MITM) attacks.
Answer: C (LEAVE A REPLY)
Opportunistic Wireless Encryption (OWE) is a WPA3 feature designed for open wireless networks, where no password or authentication is required to connect. OWE enhances security by providing encryption for devices that support it, without requiring a pre-shared key (PSK) or 802.1X authentication.

Option C, "It allows anyone to connect, but provides better protection against eavesdropping than a traditional open network," is correct. In a traditional open network (no encryption), all traffic is sent in plaintext, making it vulnerable to eavesdropping. OWE allows anyone to connect (as it's an open network), but it negotiates unique encryption keys for each client using a Diffie-Hellman key exchange. This ensures that client traffic is encrypted with AES (e.g., using AES-GCMP), protecting it from eavesdropping. OWE in transition mode also supports non-OWE devices, which connect without encryption, but OWE-capable devices benefit from the added security.
Option A, "It allows both WPA2-capable and WPA3-capable clients to authenticate to the same WPA-Personal WLAN," is incorrect. OWE is for open networks, not WPA-Personal (which uses a PSK). WPA2/WPA3 transition mode (not OWE) allows both WPA2 and WPA3 clients to connect to the same WPA-Personal WLAN.
Option B, "It offers more control over who can connect to the wireless network when compared with WPA2-Personal," is incorrect. OWE is an open network protocol, meaning it offers less control over who can connect compared to WPA2-Personal, which requires a PSK for access.
Option D, "It provides protection for wireless clients against both honeypot APs and man-in-the-middle (MITM) attacks," is incorrect. OWE provides encryption to prevent eavesdropping, but it does not protect against honeypot APs (rogue APs broadcasting the same SSID) or MITM attacks, as it lacks authentication mechanisms to verify the AP's identity. Protection against such attacks requires 802.1X authentication (e.g., WPA3-Enterprise) or other security measures.
The HPE Aruba Networking AOS-8 8.11 User Guide states:
"Opportunistic Wireless Encryption (OWE) is a WPA3 feature for open networks that allows anyone to connect without a password, but provides better protection against eavesdropping than a traditional open network. OWE uses a Diffie-Hellman key exchange to negotiate unique encryption keys for each client, ensuring that traffic is encrypted with AES-GCMP and protected from unauthorized interception." (Page 290, OWE Overview Section) Additionally, the HPE Aruba Networking Wireless Security Guide notes:
"OWE enhances security for open WLANs by providing encryption without requiring authentication. It allows any device to connect, but OWE-capable devices benefit from encrypted traffic, offering better protection against eavesdropping compared to a traditional open network where all traffic is sent in plaintext." (Page 35, OWE Benefits Section)
:
HPE Aruba Networking AOS-8 8.11 User Guide, OWE Overview Section, Page 290.
HPE Aruba Networking Wireless Security Guide, OWE Benefits Section, Page 35.

NEW QUESTION: 34
Your HPE Aruba Networking Mobility Master-based solution has detected a rogue AP. Among other information, the AOS Detected Radios page lists this information for the AP:
SSID = PublicWiFi
BSSID = a8:bd:27:12:34:56
Match method = Plus one
Match method = Eth-Wired-Mac-Table

The security team asks you to explain why this AP is classified as a rogue. What should you explain?

A. The AP has been detected using multiple MAC addresses. This indicates that the AP is spoofing its MAC address, which qualifies it as a suspected rogue.

B. The AP is probably connected to your LAN because it has a BSSID that is close to a MAC address that has been detected in your LAN. Because it does not belong to the company, it is a suspected rogue.

C. The AP is an AP that belongs to your solution. However, the AOS has detected that it is behaving suspiciously. It might have been compromised, so it is classified as a suspected rogue.

D. The AP has a BSSID that is close to your authorized APs' BSSIDs. This indicates that the AP might be spoofing the corporate SSID and attempting to lure clients to it, making the AP a suspected rogue.

Answer: B (LEAVE A REPLY)

HPE Aruba Networking's Wireless Intrusion Prevention (WIP) system, part of the AOS-8 architecture (Mobility Master and Mobility Controllers), is designed to detect and classify rogue APs. The "AOS Detected Radios" page provides details about detected APs, including their SSID, BSSID, and match methods used to classify them.

In this case, the AP is classified as a rogue with the following match methods:

Plus one: This indicates that the BSSID of the detected AP is numerically close (e.g., differs by one in the last octet) to the MAC address of a known device in the network.

Eth-Wired-Mac-Table: This indicates that the AP's MAC address (or a closely related MAC address) was found in the wired network's MAC address table, suggesting that the AP is connected to the LAN.

These match methods suggest that the AP is likely connected to the company's wired LAN (via the Eth-Wired-Mac-Table match) and has a BSSID that is close to a known device's MAC address (Plus one match). Since this AP is not part of the company's authorized AP list (it's broadcasting "PublicWiFi," which may not be a corporate SSID), it is classified as a suspected rogue. This scenario is common when an unauthorized AP is plugged into the corporate LAN, posing a security risk.

Option A, "The AP has been detected using multiple MAC addresses," is incorrect because the match methods do not indicate multiple MAC addresses; they indicate a close match to a known MAC and a presence in the wired MAC table.

Option C, "The AP is an AP that belongs to your solution," is incorrect because the AP is classified as a rogue, meaning it is not part of the authorized APs in the solution.

Option D, "The AP has a BSSID that is close to your authorized APs' BSSIDs," is partially correct in that the "Plus one" match indicates a close BSSID, but the key reason for the rogue classification is its connection to the LAN (Eth-Wired-Mac-Table), not just the BSSID similarity.

The HPE Aruba Networking AOS-8 8.11 User Guide states:

"The Wireless Intrusion Prevention (WIP) system detects rogue APs by analyzing their BSSIDs, SSIDs, and connectivity to the wired network. The 'Eth-Wired-Mac-Table' match method indicates that the AP's MAC address (or a closely related address) was found in the wired network's MAC

address table, suggesting that the AP is connected to the LAN. The 'Plus one' match method indicates that the AP's BSSID is numerically close to a known MAC address in the network, which can indicate a potential rogue device attempting to mimic a legitimate device." (Page 412, Rogue AP Detection Section) Additionally, the guide notes:
"A rogue AP is classified as 'suspected rogue' if it is detected on the wired network (e.g., via Eth-Wired-Mac-Table) and is not part of the authorized AP list. This often occurs when an unauthorized AP is connected to the corporate LAN." (Page 413, Rogue AP Classification Section)
:
HPE Aruba Networking AOS-8 8.11 User Guide, Rogue AP Detection Section, Page 412.
HPE Aruba Networking AOS-8 8.11 User Guide, Rogue AP Classification Section, Page 413.

NEW QUESTION: 35
A company has an AOS controller-based solution with a WPA3-Enterprise WLAN, which authenticates wireless clients to HPE Aruba Networking ClearPass Policy Manager (CPPM). The company has decided to use digital certificates for authentication. A user's Windows domain computer has had certificates installed on it. However, the Networks and Connections window shows that authentication has failed for the user. The Mobility Controller's (MC's) RADIUS events show that it is receiving Access-Rejects for the authentication attempt.
What is one place that you can look for deeper insight into why this authentication attempt is failing?
A. The reports generated by HPE Aruba Networking ClearPass Insight
B. The RADIUS events within the CPPM Event Viewer
C. The Alerts tab in the authentication record in CPPM Access Tracker
D. The packets captured on the MC control plane destined to UDP 1812
Answer: (SHOW ANSWER)
The scenario involves an AOS-8 controller-based solution with a WPA3-Enterprise WLAN using HPE Aruba Networking ClearPass Policy Manager (CPPM) for authentication. The company is using digital certificates for authentication (likely EAP-TLS, as it's the most common certificate-based method for WPA3-Enterprise). A user's Windows domain computer has certificates installed, but authentication fails. The Mobility Controller (MC) logs show Access-Rejects from CPPM, indicating that CPPM rejected the authentication attempt.
Access-Reject: An Access-Reject message from CPPM means that the authentication failed due to a policy violation, certificate issue, or other configuration mismatch. To troubleshoot, we need to find detailed information about why CPPM rejected the request.
Option C, "The Alerts tab in the authentication record in CPPM Access Tracker," is correct. Access Tracker in CPPM logs all authentication attempts, including successful and failed ones. For a failed attempt (Access-Reject), the authentication record in Access Tracker will include an Alerts tab that provides detailed reasons for the failure. For example, if the client's certificate is invalid (e.g., expired, not trusted, or missing a required attribute), or if the user does not match a

policy in CPPM, the Alerts tab will specify the exact issue (e.g., "Certificate not trusted," "User not found in directory").
Option A, "The reports generated by HPE Aruba Networking ClearPass Insight," is incorrect. ClearPass Insight is used for generating reports and analytics (e.g., trends, usage patterns), not for real-time troubleshooting of specific authentication failures.
Option B, "The RADIUS events within the CPPM Event Viewer," is incorrect. The Event Viewer logs system-level events (e.g., service crashes, NAD mismatches), not detailed authentication failure reasons. While it might log that an Access-Reject was sent, it won't provide the specific reason for the rejection.
Option D, "The packets captured on the MC control plane destined to UDP 1812," is incorrect. Capturing packets on the MC control plane for UDP 1812 (RADIUS authentication port) can show the RADIUS exchange, but it won't provide the detailed reason for the Access-Reject. The MC logs already show the Access-Reject, so the issue lies on the CPPM side, and Access Tracker provides more insight.
The HPE Aruba Networking ClearPass Policy Manager 6.11 User Guide states:
"Access Tracker (Monitoring > Live Monitoring > Access Tracker) logs all authentication attempts, including failed ones. For an Access-Reject, the authentication record in Access Tracker includes an Alerts tab that provides detailed reasons for the failure. For example, in a certificate-based authentication (e.g., EAP-TLS), the Alerts tab might show 'Certificate not trusted' if the client's certificate is not trusted by ClearPass, or 'User not found' if the user does not match a policy. This is the primary place to look for deeper insight into authentication failures." (Page 299, Access Tracker Troubleshooting Section) Additionally, the HPE Aruba Networking AOS-8 8.11 User Guide notes:
"If the Mobility Controller logs show an Access-Reject from the RADIUS server (e.g., ClearPass), check the RADIUS server's authentication logs for details. In ClearPass, the Access Tracker provides detailed failure reasons in the Alerts tab of the authentication record, such as certificate issues or policy mismatches." (Page 500, Troubleshooting 802.1X Authentication Section)
:
HPE Aruba Networking ClearPass Policy Manager 6.11 User Guide, Access Tracker Troubleshooting Section, Page 299.
HPE Aruba Networking AOS-8 8.11 User Guide, Troubleshooting 802.1X Authentication Section, Page 500.

NEW QUESTION: 36
What is a guideline for creating certificate signing requests (CSRs) and deploying server Certificates on ArubaOS Mobility Controllers (MCs)?
A. Create the CSR online using the MC Web Ul if your company requires you to archive the private key.
B. if you create the CSR and public/private Keypair offline, create a matching private key online on the MC.

C. Create the CSR and public/private keypair offline If you want to install the same certificate on multiple MCs.
D. Generate the private key online, but the public key and CSR offline, to install the same certificate on multiple MCs.
Answer: C (LEAVE A REPLY)
Creating the Certificate Signing Request (CSR) and the public/private keypair offline is recommended when deploying server certificates on multiple ArubaOS Mobility Controllers (MCs). This method enhances security by minimizing the exposure of private keys. By creating and handling these components offline, administrators can maintain better control over the keys and ensure their security before deploying them across multiple devices. This approach also simplifies the management of certificates on multiple controllers, as the same certificate can be installed more securely and efficiently.References:
ArubaOS documentation on CSR creation and certificate management.

NEW QUESTION: 37
A company has AOS-CX switches deployed in a two-tier topology that uses OSPF routing at the core.
You need to prevent ARP poisoning attacks. To meet this need, what is one technology that you could apply to user VLANs on access layer switches? (Select two.)
A. ARP inspection
B. OSPF passive interface
C. BPDU guard (protection)
D. DHCPv4 snooping
E. BPDU filtering
Answer: A,D (LEAVE A REPLY)
The scenario involves AOS-CX switches in a two-tier topology (access and core layers) using OSPF routing at the core. The goal is to prevent ARP poisoning attacks on user VLANs at the access layer switches, where end-user devices connect. ARP poisoning (also known as ARP spoofing) is an attack where a malicious device sends fake ARP messages to associate its MAC address with the IP address of another device (e.g., the default gateway), allowing the attacker to intercept traffic.
ARP Inspection (Dynamic ARP Inspection, DAI): This feature prevents ARP poisoning by validating ARP packets against a trusted database of IP-to-MAC bindings. On AOS-CX switches, ARP inspection uses the DHCP snooping binding table to verify that ARP messages come from legitimate devices. If an ARP packet does not match the binding table, it is dropped.
DHCPv4 Snooping: This feature protects against rogue DHCP servers and builds a binding table of legitimate IP-to-MAC mappings by snooping DHCP traffic. The binding table is used by ARP inspection to validate ARP packets. DHCP snooping must be enabled before ARP inspection can function effectively, as it provides the trusted data for validation.
Option A, "ARP inspection," is correct. ARP inspection (DAI) directly prevents ARP poisoning by ensuring that ARP packets are legitimate, making it a key technology for this purpose.

Option B, "OSPF passive interface," is incorrect. OSPF passive interface is used to prevent OSPF from sending routing updates on specific interfaces, typically to reduce routing protocol traffic on user-facing interfaces. It does not prevent ARP poisoning, which is a Layer 2 attack.
Option C, "BPDU guard (protection)," is incorrect. BPDU guard protects against spanning tree protocol (STP) attacks by disabling a port if it receives BPDUs (e.g., from an unauthorized switch). It does not address ARP poisoning, which is unrelated to STP.
Option D, "DHCPv4 snooping," is correct. DHCP snooping is a prerequisite for ARP inspection, as it builds the binding table used to validate ARP packets. It also protects against rogue DHCP servers, which can indirectly contribute to ARP poisoning by assigning incorrect IP addresses.
Option E, "BPDU filtering," is incorrect. BPDU filtering prevents a port from sending or receiving BPDUs, which can be used to protect against STP attacks, but it does not prevent ARP poisoning.
The HPE Aruba Networking AOS-CX 10.12 Security Guide states:
"To prevent ARP poisoning attacks on user VLANs, enable Dynamic ARP Inspection (DAI) on access layer switches. DAI validates ARP packets against the DHCP snooping binding table to ensure they come from legitimate devices. Use the command ip arp inspection vlan <vlan-list> to enable DAI on the specified VLANs. DHCP snooping must be enabled first with dhcp-snooping and dhcp-snooping vlan <vlan-list> to build the binding table used by DAI." (Page 145, ARP Inspection and DHCP Snooping Section) Additionally, the guide notes:
"DHCP snooping and ARP inspection work together to protect against Layer 2 attacks like ARP poisoning. DHCP snooping builds a trusted database of IP-to-MAC bindings, which ARP inspection uses to filter out malicious ARP packets." (Page 146, Best Practices Section)
:
HPE Aruba Networking AOS-CX 10.12 Security Guide, ARP Inspection and DHCP Snooping Section, Page 145.
HPE Aruba Networking AOS-CX 10.12 Security Guide, Best Practices Section, Page 146.

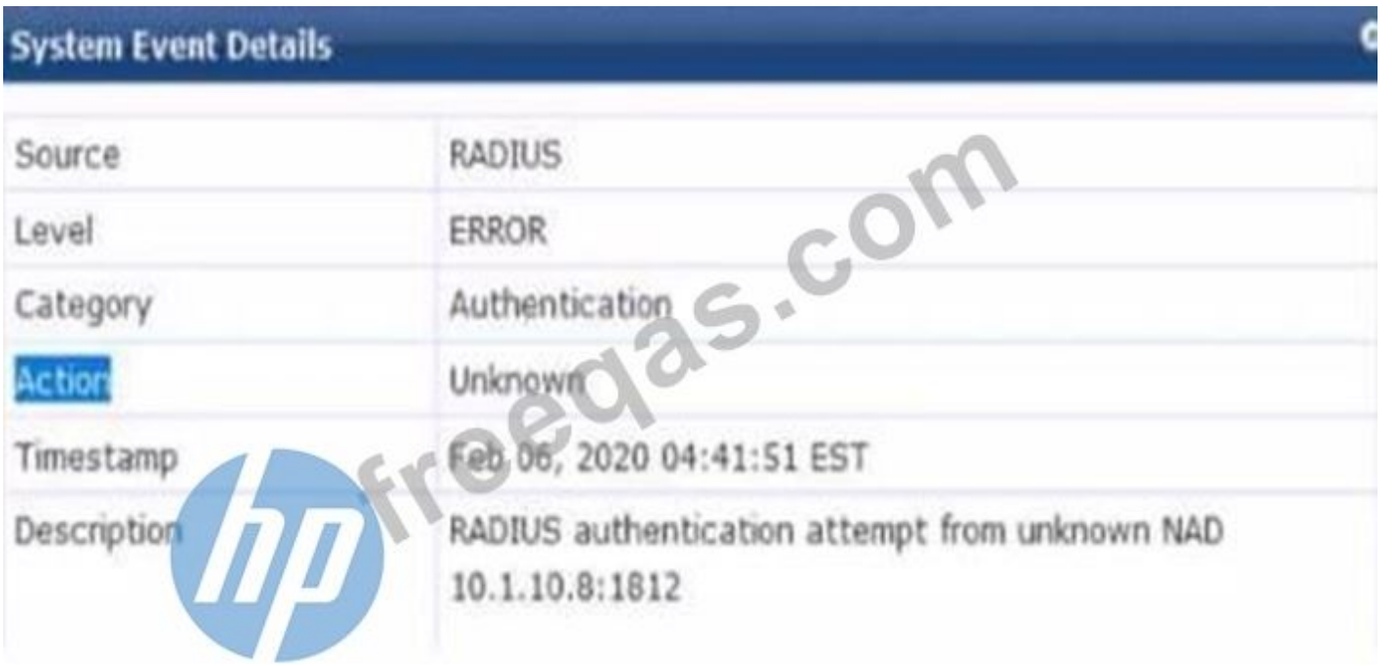
NEW QUESTION: 38
Refer to the exhibit, which shows the settings on the company's MCs.

- Mobility Controller
Dashboard General Admin AirWave CPSec Certificates
Configuration
WLANsv Control Plane Security

Roles & PoliciesEnable CP Sec
Access PointsEnable auto cert provisioning:
You have deployed about 100 new Aruba 335-APs. What is required for the APs to become managed?
A. installing CA-signed certificates on the APs
B. installing self-signed certificates on the APs
C. approving the APs as authorized APs on the AP whitelist
D. configuring a PAPI key that matches on the APs and MCs
Answer: (SHOW ANSWER)
Based on the exhibit, which shows the settings on the company's Mobility Controllers (MCs), with 'Control Plane Security' enabled and 'Enable auto cert provisioning' available, new Aruba 335-APs require approval on the MC to become managed. This is commonly done by adding the APs to an authorized AP whitelist, after which they can be automatically provisioned with certificates generated by the MC.

NEW QUESTION: 39
What distinguishes a Distributed Denial of Service (DDoS) attack from a traditional Denial or service attack (DoS)?
A. A DDoS attack originates from external devices, while a DoS attack originates from internal devices
B. A DDoS attack is launched from multiple devices, while a DoS attack is launched from a single device
C. A DoS attack targets one server, a DDoS attack targets all the clients that use a server
D. A DDoS attack targets multiple devices, while a DoS Is designed to Incapacitate only one device
Answer: B (LEAVE A REPLY)
The main distinction between a Distributed Denial of Service (DDoS) attack and a traditional Denial of Service (DoS) attack is that a DDoS attack is launched from multiple devices, whereas a DoS attack originates from a single device. This distinction is critical because the distributed nature of a DDoS attack makes it more difficult to mitigate. Multiple attacking sources can generate a higher volume of malicious traffic, overwhelming the target more effectively than a single source, as seen in a DoS attack. DDoS attacks exploit a variety of devices across the internet, often coordinated using botnets, to flood targets with excessive requests, leading to service degradation or complete service denial.
References:
Cybersecurity texts and resources that differentiate between types of denial of service attacks.
Technical documentation and analysis of DDoS tactics, which illustrate how botnets and other distributed systems are employed to execute attacks.

NEW QUESTION: 40
Refer to the exhibit.



You are deploying a new ArubaOS Mobility Controller (MC), which is enforcing authentication to Aruba ClearPass Policy Manager (CPPM). The authentication is not working correctly, and you find the error shown In the exhibit in the CPPM Event Viewer.

What should you check?

A. that the MC has valid admin credentials configured on it for logging into the CPPM

B. that the MC has been added as a domain machine on the Active Directory domain with which CPPM is synchronized

C. that the IP address that the MC is using to reach CPPM matches the one defined for the device on CPPM

D. that the snared secret configured for the CPPM authentication server matches the one defined for the device on CPPM

Answer: C (LEAVE A REPLY)

NEW QUESTION: 41

Two wireless clients, client 1 and client 2, are connected to an ArubaOS Mobility Controller. Subnet

10.1.10.10/24 is a network of servers on the other side of the ArubaOS firewall. The exhibit shows all three firewall rules that apply to these clients.

Refer to the exhibit.

Which traffic is permitted?

A. an HTTPS request from client 1 to 10.1.10.10 and an HTTPS response from 10.1.10.10 to client 1

B. an HTTPS request from client 1 to 10.1.10.10 and an HTTPS request from 10.1.10.11 to client 1

C. an HTTPS request from 10.1.10.10 to client 1 and an HTTPS re-sponse from client 1 to 10.1.10.10

D. an HTTPS request from client 1 to client 2 and an HTTPS request from client 2 to client 1

Answer: (SHOW ANSWER)

Based on the exhibit showing the firewall rules, the following traffic is permitted:

Client 1 is allowed to send HTTPS traffic to any destination within the subnet 10.1.10.0/24 because there is a permit rule for the user to access svc-https to that subnet.

Responses to initiated connections are typically allowed by stateful firewalls; hence, an HTTPS response from 10.1.10.10 to client 1 is expected to be permitted even though it is not explicitly mentioned in the firewall rules (assuming the stateful nature of the firewall).

NEW QUESTION: 42

You have detected a Rogue AP using the Security Dashboard Which two actions should you take in responding to this event? (Select two)

A. There is no need to locale the AP If you manually contain It.

B. This is a serious security event, so you should always contain the AP immediately regardless of your company's specific policies.

C. You should receive permission before containing an AP. as this action could have legal Implications.

D. For forensic purposes, you should copy out logs with relevant information, such as the time mat the AP was detected and the AP's MAC address.

E. There is no need to locate the AP If the Aruba solution is properly configured to automatically contain it.

Answer: C,D (LEAVE A REPLY)

When responding to the detection of a Rogue AP, it's important to consider legal implications and to gather forensic evidence:

You should receive permission before containing an AP (Option C), as containing it could disrupt service and may have legal implications, especially if the AP is on a network that the organization does not own.

For forensic purposes, it is essential to document the event by copying out logs with relevant information, such as the time the AP was detected and the AP's MAC address (Option D). This information could be crucial if legal action is taken or if a detailed analysis of the security breach is required.

Automatically containing an AP without consideration for the context (Options A and E) can be problematic, as it might inadvertently interfere with neighboring networks and cause legal issues.

Immediate containment without consideration of company policy (Option B) could also violate established incident response procedures.

References:

Aruba Networks security resources that discuss the appropriate steps in responding to security events.

Industry guidelines on responsible handling of rogue access point detections, including legal considerations and incident documentation.

NEW QUESTION: 43

You configure an ArubaOS-Switch to enforce 802.1X authentication with ClearPass Policy Manager (CPPM) denned as the RADIUS server Clients cannot authenticate You check Aruba ClearPass Access Tracker and cannot find a record of the authentication attempt.

What are two possible problems that have this symptom? (Select two)

A. users are logging in with the wrong usernames and passwords or invalid certificates.

B. Clients are configured to use a mismatched EAP method from the one In the CPPM service.

C. The RADIUS shared secret does not match between the switch and CPPM.

D. CPPM does not have a network device defined for the switch's IP address.

E. Clients are not configured to trust the root CA certificate for CPPM's RADIUS/EAP certificate.

Answer: C,D (LEAVE A REPLY)

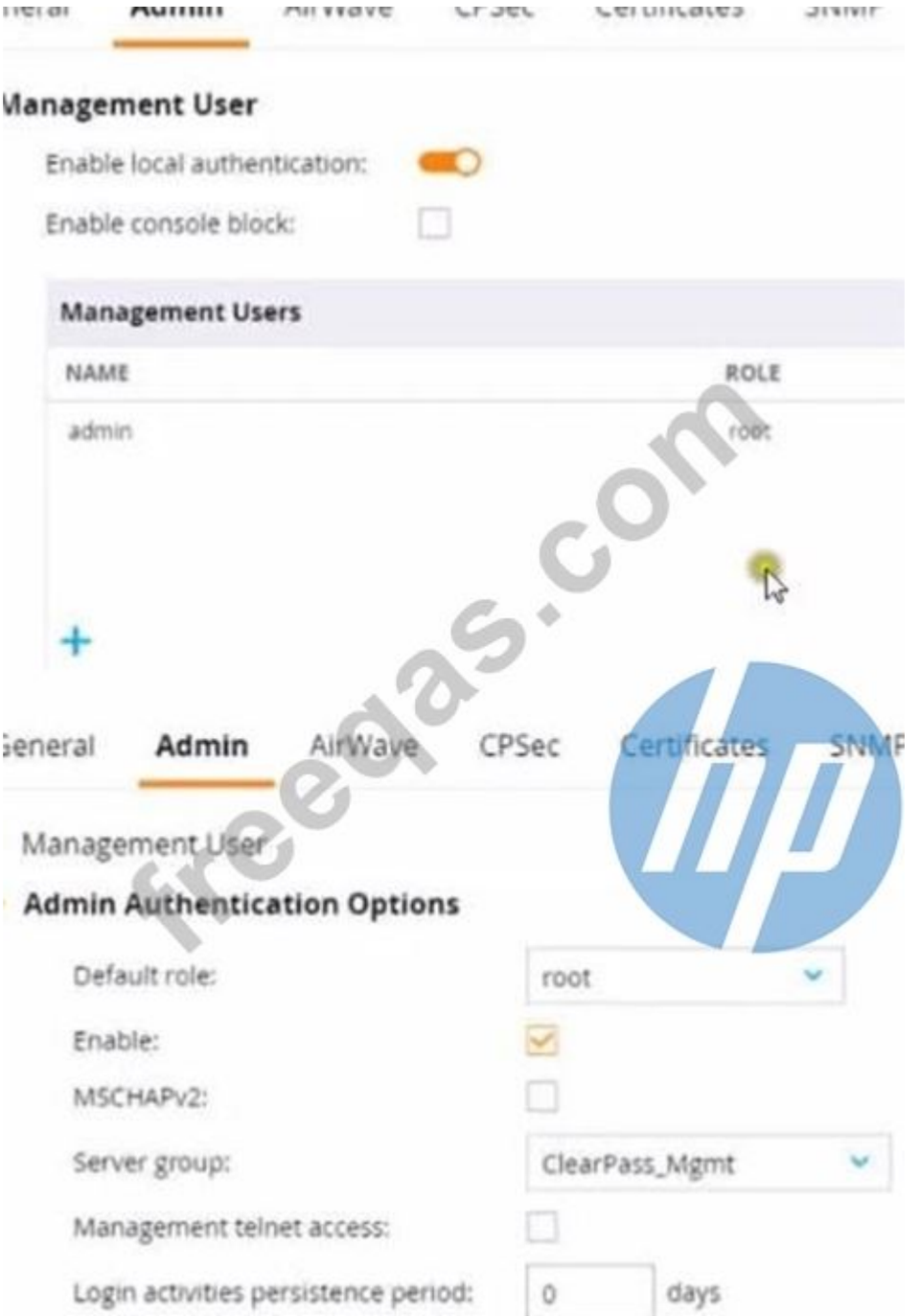
If clients cannot authenticate and there is no record of the authentication attempt in Aruba ClearPass Access Tracker, two possible problems that could cause this symptom are:

The RADIUS shared secret does not match between the switch and CPPM. This mismatch would prevent the switch and CPPM from successfully communicating, so authentication attempts would fail, and no record would appear in Access Tracker.

CPPM does not have a network device profile defined for the switch's IP address. Without a network device profile, CPPM would not recognize authentication attempts coming from the switch and would not process them, resulting in no logs in Access Tracker.

The other options are incorrect because:
Users logging in with the wrong credentials would still generate an attempt record in Access Tracker.
Clients configured to use a mismatched EAP method would also generate an attempt record in Access Tracker.
Clients not configured to trust the root CA certificate for CPPM's RADIUS/EAP certificate might fail authentication, but the attempt would still be logged in Access Tracker.

NEW QUESTION: 44
Refer to the exhibit.



This Aruba Mobility Controller (MC) should authenticate managers who access the Web UI to ClearPass Policy Manager (CPPM) ClearPass admins have asked you to use RADIUS and

explained that the MC should accept managers' roles in Aruba-Admin-Role VSAs Which setting should you change to follow Aruba best security practices?
A. Disable local authentication
B. Change the default role to "guest-provisioning"
C. Change the local user role to read-only
D. Clear the MSCHAP check box
Answer: B (LEAVE A REPLY)

NEW QUESTION: 45
You have a network with ArubaOS-Switches for which Aruba ClearPass Policy Manager (CPPM) is acting as a TACACS+ server to authenticate managers. CPPM assigns the admins a TACACS + privilege level, either manager or operator. You are now adding ArubaOS-CX switches to the network. ClearPass admins want to use the same CPPM service and policies to authenticate managers on the new switches.
What should you explain?
A. This approach cannot work because the ArubaOS-CX switches do not accept standard TACACS+ privilege levels.
B. This approach cannot work because the ArubaOS-CX switches do not support TACACS+.
C. This approach will work, but will need to be adjusted later if you want to assign managers to the default auditors group.
D. This approach will work to assign admins to the default "administrators" group, but not to the default "operators" group.
Answer: (SHOW ANSWER)
With ArubaOS-CX switches, the use of ClearPass Policy Manager (CPPM) as a TACACS+ server for authentication is supported. The privilege levels assigned by CPPM will translate onto the switches, where the "manager" privilege level typically maps to administrative capabilities and the "operator" privilege level maps to more limited capabilities. ArubaOS-CX does support standard TACACS+ privilege levels, so administrators can be assigned appropriately. If the ClearPass policies are correctly configured, they will work for both ArubaOS-Switches and ArubaOS-CX switches. The distinction between the "administrators" and "operators" groups is inherent in the ArubaOS-CX role-based access control, and these default groups need to be appropriately mapped to the TACACS+ privilege levels assigned by CPPM.

NEW QUESTION: 46
A company has Aruba Mobility Controllers (MCs), Aruba campus APs, and ArubaOS-Switches. The company plans to use ClearPass Policy Manager (CPPM) to classify endpoints by type. This company is using only CPPM and no other ClearPass solutions.
The ClearPass admins tell you that they want to use HTTP User-Agent strings to help classify endpoints.
What should you do as a part of configuring the ArubaOS-Switches to support this requirement?
A. Create a device fingerprinting policy that includes HTTP, and apply the policy to edge ports.

B. Create remote mirrors that collect traffic on edge ports, and mirror it to CPPM's IP address.
C. Configure CPPM as the sFlow collector, and make sure that sFlow is enabled on edge ports.
D. Connect the switches to CPPM's span ports, and set up mirroring of HTTP traffic on the switches.
Answer: C (LEAVE A REPLY)
ArubaOS-Switches can use sFlow technology to sample network traffic and send the samples to a collector, such as ClearPass Policy Manager (CPPM), for analysis. sFlow can be configured to capture various types of traffic, including HTTP, which typically contains User-Agent strings that can be used for device fingerprinting and classification.
To support the requirement for using HTTP User-Agent strings to classify endpoints, the switches would need to be configured to send sFlow samples containing HTTP traffic to CPPM. CPPM would then analyze these samples and use the User-Agent strings to classify the devices.
Therefore, the correct action to configure ArubaOS-Switches would involve:
Configuring CPPM as the sFlow collector on the switches.
Enabling sFlow on the edge ports that connect to endpoints.
This approach allows the network traffic to be analyzed by CPPM without requiring any additional mirroring or redirection of traffic, which would be resource-intensive and potentially disruptive to network performance.

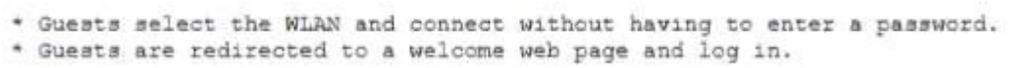
NEW QUESTION: 47
What is one of the roles of the network access server (NAS) in the AAA framewonx?
A. It authenticates legitimate users and uses policies to determine which resources each user is allowed to access.
B. It negotiates with each user's device to determine which EAP method is used for authentication
C. It enforces access to network services and sends accounting information to the AAA server
D. It determines which resources authenticated users are allowed to access and monitors each users session
Answer: C (LEAVE A REPLY)
In the AAA (Authentication, Authorization, and Accounting) framework, the role of the Network Access Server (NAS) is to act as a gateway that enforces access to network services and sends accounting information to the AAA server. The NAS initially requests authentication information

from the user and then passes that information to the AAA server. It also enforces the access policies as provided by the AAA server after authentication and provides accounting data to the AAA server based on user activity.
:
Technical literature on AAA protocols which often includes a description of the roles and responsibilities of a Network Access Server.
Network security resources that discuss the NAS function within the AAA framework.

NEW QUESTION: 48
What is a use case for tunneling traffic between an Aruba switch and an AruDa Mobility Controller (MC)?
A. applying firewall policies and deep packet inspection to wired clients
B. enhancing the security of communications from the access layer to the core with data encryption
C. securing the network infrastructure control plane by creating a virtual out-of-band-management network
D. simplifying network infrastructure management by using the MC to push configurations to the switches
Answer: (SHOW ANSWER)
Tunneling traffic between an Aruba switch and an Aruba Mobility Controller (MC) allows for the centralized application of firewall policies and deep packet inspection to wired clients. By directing traffic through the MC, network administrators can implement a consistent set of security policies across both wired and wireless segments of the network, enhancing overall network security posture.

NEW QUESTION: 49
What role does the Aruba ClearPass Device Insight Analyzer play in the Device Insight architecture?
A. It resides In the cloud and applies machine learning and supervised crowdsourcing to metadata sent by Collectors
B. It resides in the cloud and manages licensing and configuration for Collectors
C. It resides on-prem and provides the span port to which traffic is mirrored for deep analytics.
D. It resides on-prem and is responsible for running active SNMP and Nmap scans
Answer: (SHOW ANSWER)

NEW QUESTION: 50
A company with 382 employees wants to deploy an open WLAN for guests. The company wants the experience to be as follows:



The company also wants to provide encryption for the network for devices mat are capable, you implement Tor the WLAN?
Which security options should
A. WPA3-Personal and MAC-Auth
B. Captive portal and WPA3-Personai
C. Captive portal and Opportunistic Wireless Encryption (OWE) in transition mode
D. Opportunistic Wireless Encryption (OWE) and WPA3-Personal
Answer: C (LEAVE A REPLY)
For a company that wants to deploy an open WLAN for guests with the ease of access and encryption for capable devices, using a captive portal with Opportunistic Wireless Encryption (OWE) in transition mode would be suitable. The captive portal allows for a user-friendly login page for authentication without a pre-shared key, and OWE provides encryption to protect user data without the complexities of traditional WPA or WPA2 encryption, which is ideal for guest networks. Transition mode allows devices that support OWE to use it while still allowing older or unsupported devices to connect.References:
Wi-Fi Alliance recommendations for OWE.
Best practices for guest Wi-Fi network setup.

NEW QUESTION: 51
Which attack is an example or social engineering?
A. An email Is used to impersonate a Dank and trick users into entering their bank login information on a fake website page.
B. A user visits a website and downloads a file that contains a worm, which sell-replicates throughout the network.
C. An attack exploits an operating system vulnerability and locks out users until they pay the ransom.
D. A hacker eavesdrops on insecure communications, such as Remote Desktop Program (RDP). and discovers login credentials.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 52
What is one difference between EAP-Tunneled Layer security (EAP-TLS) and Protected EAP (PEAP)?
A. EAP-TLS creates a TLS tunnel for transmitting user credentials, while PEAP authenticates the server and supplicant during a TLS handshake.
B. EAP-TLS requires the supplicant to authenticate with a certificate, hut PEAP allows the supplicant to use a username and password.
C. EAP-TLS begins with the establishment of a TLS tunnel, but PEAP does not use a TLS tunnel as part of Its process
D. EAP-TLS creates a TLS tunnel for transmitting user credentials securely while PEAP protects user credentials with TKIP encryption.

Answer: (SHOW ANSWER)
EAP-TLS and PEAP both provide secure authentication methods, but they differ in their requirements for client-side authentication. EAP-TLS requires both the client (supplicant) and the server to authenticate each other with certificates, thereby ensuring a very high level of security. On the other hand, PEAP requires a server-side certificate to create a secure tunnel and allows the client to authenticate using less stringent methods, such as a username and password, which are then protected by the tunnel. This makes PEAP more flexible in environments where client-side certificates are not feasible.
:
EAP-TLS and PEAP authentication protocols comparison.

NEW QUESTION: 53
A company has Aruba Mobility Controllers (MCs). Aruba campus APs. and ArubaOS-CX switches. The company plans to use ClearPass Policy Manager (CPPM) to classify endpoints by type The ClearPass admins tell you that they want to run Network scans as part of the solution What should you do to configure the infrastructure to support the scans?
A. Create a TA profile on the ArubaOS-Switches with the root CA certificate for ClearPass's HTTPS certificate
B. Create device fingerprinting profiles on the ArubaOS-Switches that include SNMP. and apply the profiles to edge ports
C. Create remote mirrors on the ArubaOS-Swrtches that collect traffic on edge ports, and mirror it to CPPM's IP address.
D. Create SNMPv3 users on ArubaOS-CX switches, and make sure that the credentials match those configured on CPPM
Answer: D (LEAVE A REPLY)
To configure the infrastructure to support network scans as part of the ClearPass Policy Manager (CPPM) solution, creating SNMPv3 users on ArubaOS-CX switches is necessary. Ensuring that the credentials for these SNMPv3 users match those configured on CPPM is crucial for enabling CPPM to perform network scans effectively. SNMPv3 provides a secure method for network management by offering authentication and encryption, which are essential for safely conducting scans that classify endpoints by type. This configuration allows CPPM to communicate securely with the switches and gather necessary data without compromising network security.
:
ArubaOS-CX configuration manuals that discuss SNMP settings.
Network management and security guidelines that emphasize the importance of secure SNMP configurations for network scanning and monitoring.

NEW QUESTION: 54
You have an Aruba Mobility Controller (MC). for which you are already using Aruba ClearPass Policy Manager (CPPM) to authenticate access to the Web UI with usernames and passwords You now want to enable managers to use certificates to log in to the Web UI CPPM will continue

to act as the external server to check the names in managers' certificates and tell the MC the managers' correct rote in addition to enabling certificate authentication. what is a step that you should complete on the MC?
A. install all of the managers' certificates on the MC as OCSP Responder certificates
B. Verify that the MC has the correct certificates, and add RadSec to the RADIUS server configuration for CPPM
C. Create a local admin account mat uses certificates in the account, specify the correct trusted CA certificate and external authentication
D. Verify that the MC trusts CPPM's HTTPS certificate by uploading a trusted CA certificate Also, configure a CPPM username and password on the MC
Answer: B (LEAVE A REPLY)

NEW QUESTION: 55
A company is deploying ArubaOS-CX switches to support 135 employees, which will tunnel client traffic to an Aruba Mobility Controller (MC) for the MC to apply firewall policies and deep packet inspection (DPI).
This MC will be dedicated to receiving traffic from the ArubaOS-CX switches.
What are the licensing requirements for the MC?
A. one PEF license per-switch. and one WCC license per-switch
B. one PEF license per-switch
C. one AP license per-switch. and one PEF license per-switch
D. one AP license per-switch
Answer: C (LEAVE A REPLY)

NEW QUESTION: 56
What is the purpose of an Enrollment over Secure Transport (EST) server?
A. It provides a secure central repository for private keys associated with devices' digital certificates.
B. It helps admins to avoid expired certificates with less management effort.
C. It provides a more secure alternative to private CAs at less cost than a public CA.
D. It acts as an intermediate Certification Authority (CA) that signs end-entity certificates.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 57
Refer to the exhibit.

Device A is establishing an HTTPS session with the Arubapedia web sue using Chrome. The Arubapedia web server sends the certificate shown in the exhibit What does the browser do as part of vacating the web server certificate?

A. It uses the public key in the DigCen SHA2 Secure Server CA certificate to check the certificate's signature.

B. It uses the public key in the DigCert root CA certificate to check the certificate signature

C. It uses the private key in the DigiCert SHA2 Secure Server CA to check the certificate's signature.

D. It uses the private key in the Arubapedia web site's certificate to check that certificate's signature

Answer: A (LEAVE A REPLY)

When a browser, like Chrome, is validating a web server's certificate, it uses the public key in the certificate's signing authority to verify the certificate's digital signature. In the case of the exhibit, the browser would use the public key in the DigiCert SHA2 Secure Server CA certificate to check the signature of the Arubapedia web server's certificate. This process ensures that the certificate was indeed issued by the claimed Certificate Authority (CA) and has not been tampered with.

References:

Browser security documentation and SSL/TLS standards that explain the certificate validation process.
Cybersecurity educational resources that cover the principles of public key infrastructure (PKI) and certificate validation.

NEW QUESTION: 58
What is a benefit of Opportunistic Wireless Encryption (OWE)?
A. It allows both WPA2-capabie and WPA3-capable clients to authenticate to the same WPA-Personal WLAN
B. It offers more control over who can connect to the wireless network when compared with WPA2-Personal
C. It allows anyone lo connect, but provides better protection against eavesdropping than a traditional open network
D. It provides protection for wireless clients against both honeypot APs and man-in-the-middle (MUM) attacks
Answer: (SHOW ANSWER)
The benefit of Opportunistic Wireless Encryption (OWE) is that it allows anyone to connect, but it provides better protection against eavesdropping than a traditional open network. OWE is a type of wireless security specified in the WPA3 standard that offers encrypted communication without the complexity of a full authentication process, thereby securing data on networks that would otherwise be open and unencrypted.
:
Wi-Fi Alliance specifications for WPA3 and Opportunistic Wireless Encryption (OWE).
Security whitepapers and industry articles discussing the advantages of WPA3, including OWE.

NEW QUESTION: 59
How does the ArubaOS firewall determine which rules to apply to a specific client's traffic?
A. The firewall applies every rule that includes the dent's IP address as the source.
B. The firewall applies the rules in policies associated with the client's wlan
C. The firewall applies thee rules in policies associated with the client's user role.
D. The firewall applies every rule that includes the client's IP address as the source or destination.
Answer: C (LEAVE A REPLY)
The ArubaOS firewall determines which rules to apply to a specific client's traffic based on the rules in policies associated with the client's user role. User roles are a fundamental part of ArubaOS and the firewall policies they encompass. These roles contain policies that dictate permissions and restrictions for network traffic. When a client authenticates, it is assigned a role, and the firewall enforces the rules defined within that role for the client's traffic.
:
ArubaOS firewall and user role configuration guides that explain the role-based access control and firewall policy enforcement.

Industry best practices for network access control that advocate for role-based enforcement mechanisms.

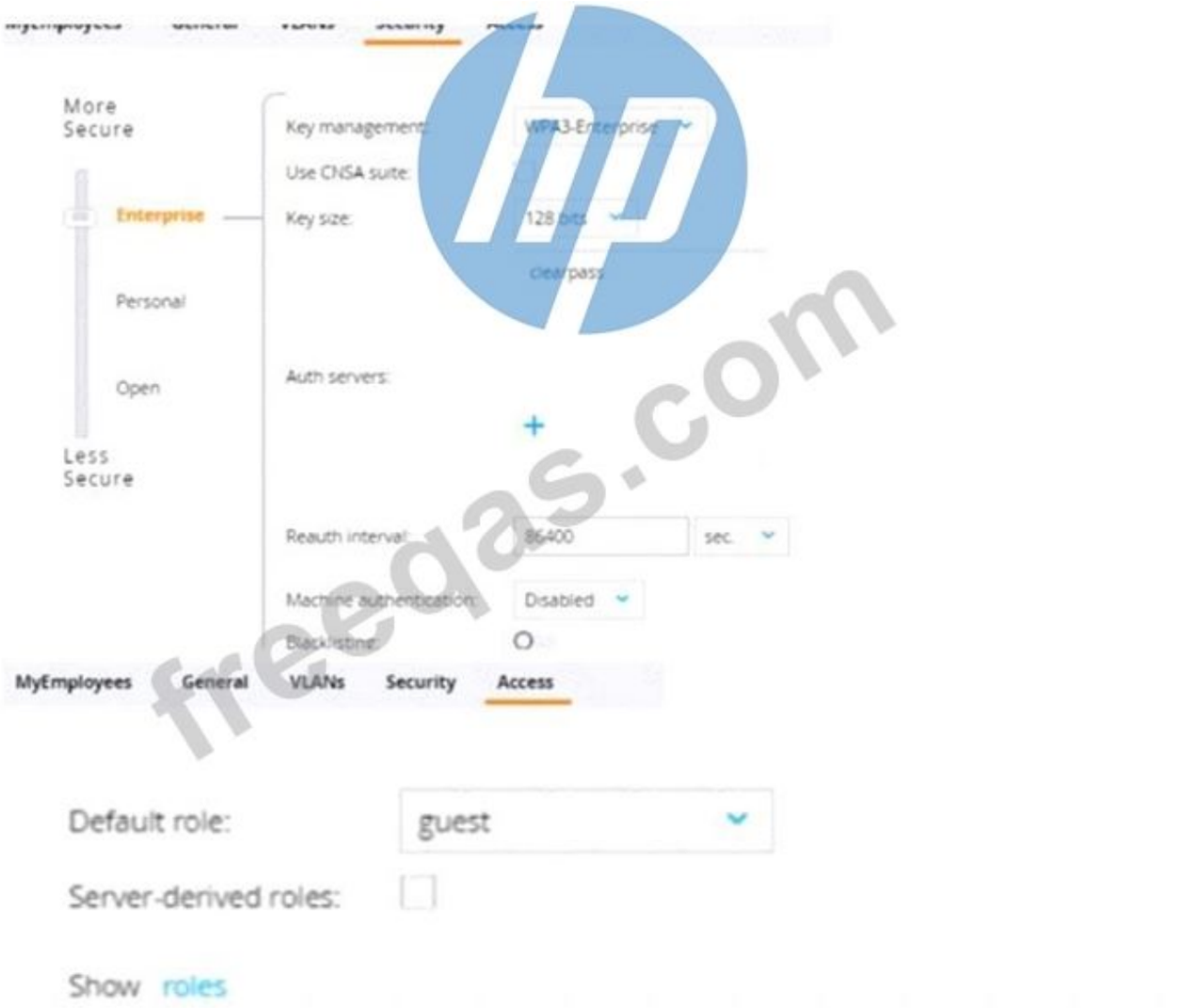
NEW QUESTION: 60
You are deploying an Aruba Mobility Controller (MC). What is a best practice for setting up secure management access to the ArubaOS Web UP
A. Avoid using external manager authentication tor the Web UI.
B. Change the default 4343 port tor the web UI to TCP 443.
C. Install a CA-signed certificate to use for the Web UI server certificate.
D. Make sure to enable HTTPS for the Web UI and select the self-signed certificate Installed in the factory.
Answer: C (LEAVE A REPLY)
For securing management access to the ArubaOS Web UI of an Aruba Mobility Controller (MC), it is a best practice to install a certificate signed by a Certificate Authority (CA). This ensures that communications between administrators and the MC are secured with trusted encryption, which greatly reduces the risk of man-in-the-middle attacks. Using a CA-signed certificate enhances the trustworthiness of the connection over self-signed certificates, which do not offer the same level of assurance.References:
ArubaOS documentation on management access security.

NEW QUESTION: 61
A company with 465 employees wants to deploy an open WLAN for guests. The company wants the experience to be as follows:
Guests select the WLAN and connect without having to enter a password.
Guests are redirected to a welcome web page and log in.
The company also wants to provide encryption for the network for devices that are capable.
Which security options should you implement for the WLAN?
A. Opportunistic Wireless Encryption (OWE) and WPA3-Personal
B. Captive portal and WPA3-Personal
C. WPA3-Personal and MAC-Auth
D. Captive portal and Opportunistic Wireless Encryption (OWE) in transition mode
Answer: D (LEAVE A REPLY)
The company wants to deploy an open WLAN for guests with the following requirements:
Guests connect without entering a password (open authentication).
Guests are redirected to a welcome web page and log in (captive portal).
Encryption is provided for devices that support it.
Open WLAN with Captive Portal: An open WLAN means no pre-shared key (PSK) or 802.1X authentication is required to connect. A captive portal can be used to redirect users to a web page where they must log in (e.g., with guest credentials). This meets the requirement for guests to connect without a password and then log in via a web page.

Encryption for Capable Devices: The company wants to provide encryption for devices that support it, even on an open WLAN. Opportunistic Wireless Encryption (OWE) is a WPA3 feature designed for open networks. OWE provides encryption without requiring a password by negotiating unique encryption keys for each client using a Diffie-Hellman key exchange. OWE in transition mode allows both OWE-capable devices (which use encryption) and non-OWE devices (which connect without encryption) to join the same SSID, ensuring compatibility.
Option A, "Opportunistic Wireless Encryption (OWE) and WPA3-Personal," is incorrect. WPA3-Personal requires a pre-shared key (password), which conflicts with the requirement for guests to connect without entering a password.
Option B, "Captive portal and WPA3-Personal," is incorrect for the same reason. WPA3-Personal requires a password, which does not meet the open WLAN requirement.
Option C, "WPA3-Personal and MAC-Auth," is incorrect. WPA3-Personal requires a password, and MAC authentication (MAC-Auth) does not provide the web-based login experience (captive portal) specified in the requirements.
Option D, "Captive portal and Opportunistic Wireless Encryption (OWE) in transition mode," is correct. An open WLAN with OWE in transition mode allows guests to connect without a password, provides encryption for OWE-capable devices (e.g., WPA3 devices), and supports non-OWE devices without encryption. The captive portal ensures that guests are redirected to a welcome web page to log in, meeting all requirements.
The HPE Aruba Networking AOS-8 8.11 User Guide states:
"Opportunistic Wireless Encryption (OWE) is a WPA3 feature that provides encryption for open WLANs without requiring a password. In OWE transition mode, the WLAN supports both OWE-capable devices (which use encryption) and non-OWE devices (which connect without encryption) on the same SSID. This is ideal for guest networks where encryption is desired for capable devices, but compatibility with all devices is required. A captive portal can be configured on an open WLAN to redirect users to a login page, such as captive-portal guest-login, ensuring a seamless guest experience." (Page 290, OWE and Captive Portal Section) Additionally, the HPE Aruba Networking Wireless Security Guide notes:
"OWE in transition mode is recommended for open guest WLANs where encryption is desired for devices that support it. Combined with a captive portal, this setup allows guests to connect without a password, get redirected to a login page, and benefit from encryption if their device supports OWE." (Page 35, Guest Network Security Section)
:
HPE Aruba Networking AOS-8 8.11 User Guide, OWE and Captive Portal Section, Page 290.
HPE Aruba Networking Wireless Security Guide, Guest Network Security Section, Page 35.

NEW QUESTION: 62

The first exhibit shows roles on the MC, listed in alphabetic order. The second and third exhibits show the configuration for a WLAN to which a client connects. Which description of the role assigned to a user under various circumstances is correct?



A. A user fails 802.1X authentication. The client remains connected, but is assigned the "guest" role.

B. A user authenticates successfully with 802.1 X. and the RADIUS Access-Accept includes an Aruba-User-Role VSA set to "employeel." The client's role is "guest."

C. A user authenticates successfully with 802.1X. and the RADIUS Access-Accept includes an Aruba-User-Role VSA set to "employee." The client's role is "guest."

D. A user authenticates successfully with 802.1X, and the RADIUS Access-Accept includes an Aruba-User-RoleVSA set to "employeel." The client's role is "employeel."

Answer: D (LEAVE A REPLY)

In a WLAN setup that uses 802.1X for authentication, the role assigned to a user is determined by the result of the authentication process. When a user successfully authenticates via 802.1X, the RADIUS server may include a Vendor-Specific Attribute (VSA), such as the Aruba-User-Role, in the Access-Accept message.

This attribute specifies the role that should be assigned to the user. If the RADIUS Access-Accept message includes an Aruba-User-Role VSA set to "employee1", the client should be assigned the "employee1" role, as per the VSA, and not the default "guest" role. The "guest" role would typically be a fallback if no other role is specified or if the authentication fails.

NEW QUESTION: 63
What is a guideline for managing local certificates on an ArubaOS-Switch?
A. Before installing the local certificate, create a trust anchor (TA) profile with the root CA certificate for the certificate that you will install
B. Install an Online Certificate Status Protocol (OCSP) certificate to simplify the process of enrolling and re-enrolling for certificate
C. Generate the certificate signing request (CSR) with a program offline, then, install both the certificate and the private key on the switch in a single file.
D. Create a self-signed certificate online on the switch because ArubaOS-Switches do not support CA-signed certificates.
Answer: (SHOW ANSWER)
When managing local certificates on an ArubaOS-Switch, a recommended guideline is to create a trust anchor (TA) profile with the root CA certificate before installing the local certificate. This step ensures that the switch can verify the authenticity of the certificate chain during SSL/TLS communications. The trust anchor profile establishes a basis of trust by containing the root CA certificate, which helps validate the authenticity of any subordinate certificates, including the local certificate installed on the switch. This process is essential for enhancing security on the network, as it ensures that encrypted communications involving the switch are based on a verified certificate hierarchy.
References:
ArubaOS-Switch security configuration guides that detail the process of certificate management, including the creation of trust anchor profiles.
Security best practices and SSL/TLS implementation guidelines that emphasize the importance of establishing trusted certificate chains for secure communications.

NEW QUESTION: 64
What is one method for HPE Aruba Networking ClearPass Policy Manager (CPPM) to use DHCP to classify an endpoint?
A. It can determine information such as the endpoint OS from the order of options listed in Option 55 of a DHCP Discover packet.
B. It can respond to a client's DHCP Discover with different DHCP Offers and then analyze the responses to identify the client OS.
C. It can snoop DHCP traffic to register the clients' IP addresses. It then knows where to direct its HTTP requests to actively probe for information about the client.
D. It can alter the DHCP Offer to insert itself as a proxy gateway. It will then be inline in the traffic flow and can apply traffic analytics to classify clients.
Answer: A (LEAVE A REPLY)
HPE Aruba Networking ClearPass Policy Manager (CPPM) uses device profiling to classify endpoints, and one of its passive profiling methods involves analyzing DHCP traffic. DHCP fingerprinting is a technique where ClearPass examines the DHCP packets sent by a client,

particularly the DHCP Discover packet, to identify the device's operating system or type based on specific attributes.
Option A, "It can determine information such as the endpoint OS from the order of options listed in Option 55 of a DHCP Discover packet," is correct. DHCP Option 55 (Parameter Request List) is a field in the DHCP Discover packet where the client specifies the list of DHCP options it requests from the server. The order and combination of these options are often unique to specific operating systems or device types (e.g., Windows, Linux, macOS, or IoT devices). ClearPass maintains a database of DHCP fingerprints and matches the Option 55 data against this database to classify the endpoint.
Option B, "It can respond to a client's DHCP Discover with different DHCP Offers and then analyze the responses," is incorrect because ClearPass does not act as a DHCP server or send DHCP Offers. It passively snoops DHCP traffic rather than actively responding to DHCP requests.
Option C, "It can snoop DHCP traffic to register the clients' IP addresses," is partially correct in that ClearPass does snoop DHCP traffic, but the purpose is not just to register IP addresses for HTTP probing. While ClearPass can use IP addresses for active probing (e.g., HTTP or SNMP), the question specifically asks about using DHCP to classify, which is done via fingerprinting, not IP registration.
Option D, "It can alter the DHCP Offer to insert itself as a proxy gateway," is incorrect because ClearPass does not modify DHCP packets or act as a proxy gateway. This is not a function of ClearPass in the context of DHCP-based profiling.
The HPE Aruba Networking ClearPass Policy Manager 6.11 User Guide states:
"ClearPass can profile devices using DHCP fingerprinting, a passive profiling method. When a device sends a DHCP Discover packet, ClearPass examines the packet's attributes, including the order of options in DHCP Option 55 (Parameter Request List). The combination and order of these options are often unique to specific operating systems or device types. ClearPass matches these attributes against its DHCP fingerprint database to classify the device (e.g., identifying a device as a Windows 10 laptop or an Android phone)." (Page 247, DHCP Fingerprinting Section)
Additionally, the ClearPass Device Insight Data Sheet notes:
"DHCP fingerprinting allows ClearPass to passively collect device information without interfering with network traffic. By analyzing DHCP Option 55, ClearPass can accurately determine the device's operating system and type, enabling precise policy enforcement." (Page 3)
:
HPE Aruba Networking ClearPass Policy Manager 6.11 User Guide, DHCP Fingerprinting Section, Page 247.
ClearPass Device Insight Data Sheet, Page 3.

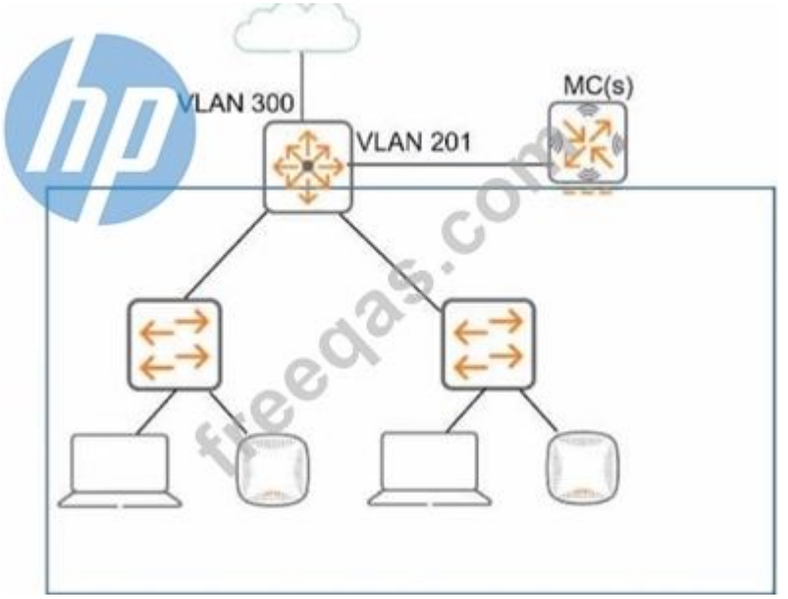
NEW QUESTION: 65
You configure an ArubaOS-Switch to enforce 802.1X authentication with ClearPass Policy Manager (CPPM) denned as the RADIUS server Clients cannot authenticate You check Aruba ClearPass Access Tracker and cannot find a record of the authentication attempt.
What are two possible problems that have this symptom? (Select two)

A. Clients are not configured to trust the root CA certificate for CPPM's RADIUS/EAP certificate.
B. The RADIUS shared secret does not match between the switch and CPPM.
C. CPPM does not have a network device defined for the switch's IP address.
D. Clients are configured to use a mismatched EAP method from the one In the CPPM service.
E. users are logging in with the wrong usernames and passwords or invalid certificates.
Answer: (SHOW ANSWER)

NEW QUESTION: 66
What distinguishes a Distributed Denial of Service (DDoS) attack from a traditional Denial or service attack (DoS)?
A. A DoS attack targets one server, a DDoS attack targets all the clients that use a server
B. A DDoS attack targets multiple devices, while a DoS Is designed to Incapacitate only one device
C. A DDoS attack is launched from multiple devices, while a DoS attack is launched from a single device
D. A DDoS attack originates from external devices, while a DoS attack originates from internal devices
Answer: D (LEAVE A REPLY)

NEW QUESTION: 67
You need to deploy an Aruba instant AP where users can physically reach It. What are two recommended options for enhancing security for management access to the AP? (Select two)
A. install a CA-signed certificate
B. Configure WPA3-Enterpnse security on the AP
C. Disable Its console ports
D. Place a Tamper Evident Label (TELS) over its console port
E. Disable the Web Ul.
Answer: A,D (LEAVE A REPLY)

NEW QUESTION: 68
Refer to the exhibit, which shows the current network topology.



You are deploying a new wireless solution with an Aruba Mobility Master (MM). Aruba Mobility Controllers (MCs). and campus APs (CAPs). The solution will Include a WLAN that uses Tunnel for the forwarding mode and Implements WPA3-Enterprise security What is a guideline for setting up the vlan for wireless devices connected to the WLAN?

A. Assign the WLAN to a single new VLAN which is dedicated to wireless users

B. Use wireless user roles to assign the devices to different VLANs in the 100-150 range

C. Assign the WLAN to a named VLAN which specified 100-150 as the range of IDs.

D. Use wireless user roles to assign the devices to a range of new vlan IDs.

Answer: B (LEAVE A REPLY)

When setting up VLANs for a wireless solution with an Aruba Mobility Master (MM), Aruba Mobility Controllers (MCs), and campus APs (CAPs), it is recommended to use wireless user roles to assign devices to different VLANs. This allows for greater flexibility and control over network resources and policies applied to different user groups. Wireless user roles can dynamically assign devices to the appropriate VLAN based on a variety of criteria such as user identity, device type, location, and the resources they need to access. This approach aligns with the ArubaOS features that leverage user roles for network access control, as detailed in Aruba's configuration and administration guides.

NEW QUESTION: 69

What is a difference between radius and TACACS+?

A. RADIUS combines the authentication and authorization process while TACACS+ separates them.

B. RADIUS uses TCP for Its connection protocol, while TACACS+ uses UDP tor its connection protocol.

C. RADIUS encrypts the complete packet, white TACACS+ only offers partial encryption.

D. RADIUS uses Attribute Value Pairs (AVPs) in its messages, while TACACS+ does not use them.

Answer: A (LEAVE A REPLY)

RADIUS and TACACS+ are both protocols used for networking authentication, but they handle the processes of authentication and authorization differently. RADIUS (Remote Authentication Dial-In User Service) combines authentication and authorization into a single process, whereas TACACS+ (Terminal Access Controller Access-Control System Plus) separates these processes. This separation in TACACS+ allows more flexible policy enforcement and better control over commands a user can execute. This difference is well-documented in various network security resources, including Cisco's technical documentation and security protocol manuals.

NEW QUESTION: 70
You have an Aruba Mobility Controller (MC). for which you are already using Aruba ClearPass Policy Manager (CPPM) to authenticate access to the Web UI with usernames and passwords You now want to enable managers to use certificates to log in to the Web UI CPPM will continue to act as the external server to check the names in managers' certificates and tell the MC the managers' correct rote in addition to enabling certificate authentication. what is a step that you should complete on the MC?
A. Verify that the MC has the correct certificates, and add RadSec to the RADIUS server configuration for CPPM
B. install all of the managers' certificates on the MC as OCSP Responder certificates
C. Verify that the MC trusts CPPM's HTTPS certificate by uploading a trusted CA certificate Also, configure a CPPM username and password on the MC
D. Create a local admin account mat uses certificates in the account, specify the correct trusted CA certificate and external authentication
Answer: C (LEAVE A REPLY)
To enable managers to use certificates to log into the Web UI of an Aruba Mobility Controller (MC), where Aruba ClearPass Policy Manager (CPPM) acts as the external server for authentication, it is essential to ensure that the MC trusts the HTTPS certificate used by CPPM. This involves uploading a trusted CA certificate to the MC that matches the one used by CPPM. Additionally, configuring a username and password for CPPM on the MC might be necessary to secure and facilitate communication between the MC and CPPM. This setup ensures that certificate-based authentication is securely validated, maintaining secure access control for the Web UI.
:
Aruba Mobility Controller configuration guides that detail the process of setting up certificate-based authentication.
Best practices for secure authentication and certificate management in enterprise network environments.

NEW QUESTION: 71
Refer to the exhibits.

An admin has created a WLAN that uses the settings shown in the exhibits (and has not otherwise adjusted the settings in the AAA profile). A client connects to the WLAN. Under which circumstances will a client receive the default role assignment?

A. The client has attempted 802.1X authentication, but the MC could not contact the authentication server.

B. The client has passed 802.1X authentication, and the authentication server did not send an Aruba-User-Role VSA.

C. The client has attempted 802.1X authentication, but failed to maintain a reliable connection, leading to a timeout error.

D. The client has passed 802.1X authentication, and the value in the Aruba-User-Role VSA matches a role on the MC.

Answer: (SHOW ANSWER)

The exhibit shows the configuration of a WLAN on an AOS-8 Mobility Controller (MC) with the following settings:

Key management: WPA3-Enterprise (indicating 802.1X authentication).

Use CNSA suite: Unchecked (using standard encryption, not the Commercial National Security Algorithm suite).

Key size: 128 bits (standard for AES-GCMP in WPA3).

Reauth interval: 1440 minutes (24 hours, the interval for re-authentication).

Machine authentication: Disabled (only user authentication is required).

Blacklisting: Disabled (clients are not blacklisted after failed attempts).

The question states that the AAA profile settings have not been adjusted, meaning the default roles (e.g., initial role, logon role, 802.1X default role) are not specified in the exhibit and are assumed to be the system defaults (e.g., "logon" for the initial and logon roles, and a default role like "guest" for the 802.1X default role). The question asks under which circumstances a client will receive the "default role assignment," which refers to the 802.1X default role configured in the AAA profile for the WLAN.

802.1X Authentication Process in AOS-8:

When a client connects to a WPA3-Enterprise WLAN, it starts in the initial role (typically "logon") to allow basic connectivity (e.g., DHCP, DNS).

During 802.1X authentication, the client is placed in the logon role to allow communication with the authentication server (e.g., ClearPass Policy Manager, CPPM).

If authentication succeeds, the client is assigned a role:

If the authentication server (e.g., CPPM) sends an Aruba-User-Role VSA with a role that exists on the MC, the client is assigned that role.

If no Aruba-User-Role VSA is sent, the client is assigned the 802.1X default role configured in the AAA profile for the WLAN.

If authentication fails or the server is unreachable, the client may be assigned a different role (e.g., a critical role, if configured) or denied access.

Option A, "The client has attempted 802.1X authentication, but the MC could not contact the authentication server," is incorrect. If the MC cannot contact the authentication server (e.g., due

to a timeout), the client does not receive the 802.1X default role. Instead, the MC may apply a critical role (if configured) or deny access, depending on the configuration. The 802.1X default role is applied only after successful authentication.
Option B, "The client has passed 802.1X authentication, and the authentication server did not send an Aruba-User-Role VSA," is correct. If the client successfully authenticates via 802.1X and the authentication server (e.g., CPPM) does not send an Aruba-User-Role VSA, the MC assigns the client the 802.1X default role configured in the AAA profile for the WLAN. This is the "default role assignment" referred to in the question.
Option C, "The client has attempted 802.1X authentication, but failed to maintain a reliable connection, leading to a timeout error," is incorrect. A timeout error during authentication (e.g., the client fails to respond to EAP messages) typically results in an authentication failure, not a successful authentication. The client would not receive the 802.1X default role; it might be denied access or placed in a different role (e.g., a pre-authentication role).
Option D, "The client has passed 802.1X authentication, and the value in the Aruba-User-Role VSA matches a role on the MC," is incorrect. If the authentication server sends an Aruba-User-Role VSA with a role that exists on the MC, the client is assigned that specific role, not the 802.1X default role.
The HPE Aruba Networking AOS-8 8.11 User Guide states:
"After a client successfully authenticates via 802.1X, the Mobility Controller assigns a role to the client. If the authentication server (e.g., a RADIUS server) sends an Aruba-User-Role VSA with a role that exists on the controller, the client is assigned that role. If no Aruba-User-Role VSA is sent in the Access-Accept message, the client is assigned the 802.1X default role configured in the AAA profile for the WLAN. For example, if the AAA profile specifies 'guest' as the 802.1X default role, the client will be assigned the 'guest' role." (Page 305, Role Assignment Section)
Additionally, the HPE Aruba Networking Wireless Security Guide notes:
"In WPA3-Enterprise with 802.1X authentication, the default role assignment occurs when a client successfully authenticates but the authentication server does not specify a role via the Aruba-User-Role VSA. In this case, the client receives the 802.1X default role defined in the AAA profile, such as 'guest' or another role configured by the administrator." (Page 42, 802.1X Role Assignment Section)
:
HPE Aruba Networking AOS-8 8.11 User Guide, Role Assignment Section, Page 305.
HPE Aruba Networking Wireless Security Guide, 802.1X Role Assignment Section, Page 42.

NEW QUESTION: 72
What is one way that WPA3-PerSonal enhances security when compared to WPA2-Personal?
A. WPA3-Personal is more complicated to deploy because it requires a backend authentication server
B. WPA3-Personai prevents eavesdropping on other users' wireless traffic by a user who knows the passphrase for the WLAN.

C. WPA3-Personai is more resistant to passphrase cracking Because it requires passphrases to be at least 12 characters
D. WPA3-Perscn3i is more secure against password leaking Because all users nave their own username and password
Answer: D (LEAVE A REPLY)

NEW QUESTION: 73
What is a vulnerability of an unauthenticated Dime-Heliman exchange?
A. A hacker can replace the public values exchanged by the legitimate peers and launch an MITM attack.
B. A brute force attack can relatively quickly derive Diffie-Hellman private values if they are able to obtain public values
C. Diffie-Hellman with elliptic curve values is no longer considered secure in modem networks, based on NIST recommendations.
D. Participants must agree on a passphrase in advance, which can limit the usefulness of Diffie-Hell man in practical contexts.
Answer: A (LEAVE A REPLY)
The vulnerability of an unauthenticated Diffie-Hellman exchange, particularly when it comes to the risk of a man-in-the-middle (MITM) attack, is a significant concern. In this scenario, a hacker can intercept the public values exchanged between two legitimate parties and substitute them with their own. This allows the attacker to decrypt or manipulate the messages passing between the two original parties without them knowing. This answer is based on the fundamental principles of how Diffie-Hellman key exchange works and its vulnerabilities without authentication mechanisms. Reference materials from cryptographic textbooks and security protocols detail these vulnerabilities, such as those found in standards and publications by organizations like NIST.

NEW QUESTION: 74
The monitoring admin has asked you to set up an AOS-CX switch to meet these criteria:
Send logs to a SIEM Syslog server at 10.4.13.15 at the standard TCP port (514) Send a log for all events at the "warning" level or above; do not send logs with a lower level than "warning" The switch did not have any "logging" configuration on it. You then entered this command:
AOS-CX(config)# logging 10.4.13.15 tcp vrf default
What should you do to finish configuring to the requirements?
A. Specify the "warning" severity level for the logging server.
B. Add logging categories at the global level.
C. Ask for the Syslog password and configure it on the switch.
D. Configure logging as a debug destination.
Answer: A (LEAVE A REPLY)

The task is to configure an AOS-CX switch to send logs to a SIEM Syslog server at IP address 10.4.13.15 using TCP port 514, with logs for events at the "warning" severity level or above (i.e., warning, error, critical, alert, emergency). The initial command entered is:
AOS-CX(config)# logging 10.4.13.15 tcp vrf default
This command configures the switch to send logs to the Syslog server at 10.4.13.15 using TCP (port 514 is the default for TCP Syslog unless specified otherwise) and the default VRF. However, this command alone does not specify the severity level of the logs to be sent, which is a requirement of the task.
Severity Level Configuration: AOS-CX switches allow you to specify the severity level for logs sent to a Syslog server. The severity levels, in increasing order of severity, are: debug, informational, notice, warning, error, critical, alert, and emergency. The requirement is to send logs at the "warning" level or above, meaning warning, error, critical, alert, and emergency logs should be sent, but debug, informational, and notice logs should not.
Option A, "Specify the 'warning' severity level for the logging server," is correct. To meet the requirement, you need to add the severity level to the logging configuration for the specific Syslog server. The command to do this is:
AOS-CX(config)# logging 10.4.13.15 severity warning
This command ensures that only logs with a severity of warning or higher are sent to the Syslog server at 10.4.13.15. Since the initial command already specified TCP and the default VRF, this additional command completes the configuration.
Option B, "Add logging categories at the global level," is incorrect. Logging categories (e.g., system, security, network) are used to filter logs based on the type of event, not the severity level. The requirement is about severity ("warning" or above), not specific categories, so this step is not necessary to meet the stated criteria.
Option C, "Ask for the Syslog password and configure it on the switch," is incorrect. Syslog servers typically do not require a password for receiving logs, and AOS-CX switches do not have a configuration option to specify a Syslog password. Authentication or encryption for Syslog (e.g., using TLS) is not mentioned in the requirements.
Option D, "Configure logging as a debug destination," is incorrect. Configuring a debug destination (e.g., using the debug command) is used to send debug-level logs to a destination (e.g., console, buffer, or Syslog), but the requirement is to send logs at the "warning" level or above, not debug-level logs. Additionally, the logging command already specifies the Syslog server as the destination.
The HPE Aruba Networking AOS-CX 10.12 System Management Guide states:
"To configure a Syslog server on an AOS-CX switch, use the logging <ip-address> [tcp | udp] [vrf <vrf-name>] command to specify the server's IP address, protocol, and VRF. To filter logs by severity, add the severity <level> option to the logging command. For example, logging 10.4.13.15 tcp severity warning sends logs with a severity of warning or higher (warning, error, critical, alert, emergency) to the Syslog server at 10.4.13.15 using TCP. The default port for TCP Syslog is 514." (Page 89, Syslog Configuration Section) Additionally, the guide notes:

"Severity levels for logging on AOS-CX switches are, in increasing order: debug, informational, notice, warning, error, critical, alert, emergency. Specifying a severity level of 'warning' ensures that only logs at that level or higher are sent to the configured destination." (Page 90, Logging Severity Levels Section)
:
HPE Aruba Networking AOS-CX 10.12 System Management Guide, Syslog Configuration Section, Page 89.
HPE Aruba Networking AOS-CX 10.12 System Management Guide, Logging Severity Levels Section, Page 90.

NEW QUESTION: 75
What are the roles of 802.1X authenticators and authentication servers?
A. The authenticator stores the user account database, while the server stores access policies.
B. The authenticator supports only EAP, while the authentication server supports only RADIUS.
C. The authenticator is a RADIUS client and the authentication server is a RADIUS server.
D. The authenticator makes access decisions and the server communicates them to the supplicant.
Answer: C (LEAVE A REPLY)
In the 802.1X network access control model, the roles of the authenticator and the authentication server are distinct yet complementary. The authenticator acts as a RADIUS client, which is a network device, like a switch or wireless access point, that directly interfaces with the client machine (supplicant). The authentication server, typically a RADIUS server, is responsible for verifying the credentials provided by the supplicant through the authenticator. This setup helps in separating the duties where the authenticator enforces authentication but does not decide on the validity of the credentials, which is the role of the authentication server.References:
IEEE 802.1X standard for network access control.

NEW QUESTION: 76
What is one practice that can help you to maintain a digital chain of custody in your network?
A. Enable packet capturing on Instant AP or Mobility Controller (MC) datapath on an ongoing basis.
B. Ensure that all network infrastructure devices use RADIUS rather than TACACS+ to authenticate managers.
C. Ensure that all network infrastructure devices receive a valid clock using authenticated NTP.
D. Enable packet capturing on Instant AP or Mobility Controller (MC) controlpath on an ongoing basis.
Answer: C (LEAVE A REPLY)
A digital chain of custody ensures that evidence (e.g., logs, timestamps) collected from a network can be reliably used in legal or forensic investigations. It requires maintaining the integrity and authenticity of data, including accurate timestamps for events. HPE Aruba Networking devices,

such as Instant APs, Mobility Controllers (MCs), and AOS-CX switches, support features to help maintain a digital chain of custody.
Option C, "Ensure that all network infrastructure devices receive a valid clock using authenticated NTP," is correct. Accurate and synchronized time across all network devices is critical for maintaining a digital chain of custody. Timestamps in logs (e.g., authentication events, traffic logs) must be consistent and verifiable. Network Time Protocol (NTP) is used to synchronize device clocks, and authenticated NTP ensures that the time source is trusted and not tampered with (e.g., using MD5 or SHA authentication). This practice ensures that logs from different devices can be correlated accurately during an investigation.
Option A, "Enable packet capturing on Instant AP or Mobility Controller (MC) datapath on an ongoing basis," is incorrect. While packet capturing on the datapath (user traffic) can provide detailed traffic data for analysis, enabling it on an ongoing basis is impractical due to storage and performance constraints. Packet captures are typically used for specific troubleshooting or investigations, not for maintaining a chain of custody.
Option B, "Ensure that all network infrastructure devices use RADIUS rather than TACACS+ to authenticate managers," is incorrect. The choice of RADIUS or TACACS+ for manager authentication does not directly impact the digital chain of custody. Both protocols can log authentication events, but the protocol used does not ensure the integrity of timestamps or evidence.
Option D, "Enable packet capturing on Instant AP or Mobility Controller (MC) controlpath on an ongoing basis," is incorrect for similar reasons as Option A. Control path (control plane) packet captures include management traffic (e.g., between APs and MCs), but enabling them continuously is not practical and does not directly contribute to maintaining a chain of custody. Accurate timestamps in logs are more relevant.
The HPE Aruba Networking Security Guide states:
"Maintaining a digital chain of custody requires ensuring the integrity and authenticity of network logs and events. A critical practice is to ensure that all network infrastructure devices, such as Mobility Controllers and AOS-CX switches, receive a valid and synchronized clock using authenticated NTP. Use the command ntp server <ip-address> key <key-id> to configure authenticated NTP, ensuring that timestamps in logs are accurate and verifiable for forensic investigations." (Page 85, Digital Chain of Custody Section) Additionally, the HPE Aruba Networking AOS-8 8.11 User Guide notes:
"Accurate time synchronization is essential for maintaining a digital chain of custody. Configure all devices to use authenticated NTP to synchronize their clocks with a trusted time source. This ensures that event logs, such as authentication and traffic logs, have consistent and reliable timestamps, which can be correlated across devices during an investigation." (Page 380, Time Synchronization Section)
:
HPE Aruba Networking Security Guide, Digital Chain of Custody Section, Page 85.
HPE Aruba Networking AOS-8 8.11 User Guide, Time Synchronization Section, Page 380.

NEW QUESTION: 77
Refer to the exhibit.

A diem is connected to an ArubaOS Mobility Controller. The exhibit snows all Tour firewall rules that apply to this diem What correctly describes how the controller treats HTTPS packets to these two IP addresses, both of which are on the other side of the firewall
10.1 10.10
203.0.13.5
A. It drops both of the packets
B. It permits the packet to 10.1.10.10 and drops the packet to 203 0.13.5
C. it permits both of the packets
D. It drops the packet to 10.1.10.10 and permits the packet to 203.0.13.5.
Answer: B (LEAVE A REPLY)
Referring to the exhibit, the ArubaOS Mobility Controller treats HTTPS packets based on the firewall rules applied to the client. The rule that allows svc-https service for destination IP range 10.1.0.0 255.255.0.0 would permit an HTTPS packet to 10.1.10.10 since this IP address falls within the specified range. There are no rules shown that would allow traffic to the IP address 203.0.13.5; hence, the packet to this address would be dropped.
References:

ArubaOS firewall configuration guides detailing how firewall rules are interpreted and applied to traffic.
Network security textbooks explaining firewall rule processing and packet filtering based on source and destination IP addresses.

NEW QUESTION: 78
What is a reason to set up a packet capture on an Aruba Mobility Controller (MC)?
A. You want the MC to analyze wireless clients' traffic at a lower level, so that the ArubaOS firewall can control the traffic I based on application.
B. The company wants to use ClearPass Policy Manager (CPPM) to profile devices and needs to receive HTTP User-Agent strings from the MC.
C. You want the MC to analyze wireless clients' traffic at a lower level, so that the ArubaOS firewall can control Web traffic based on the destination URL.
D. The security team believes that a wireless endpoint connected to the MC is launching an attack and wants to examine the traffic more closely.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 79
A company has an ArubaOS controller-based solution with a WPA3-Enterprise WLAN. which authenticates wireless clients to Aruba ClearPass Policy Manager (CPPM). The company has decided to use digital certificates for authentication A user's Windows domain computer has had certificates installed on it However, the Networks and Connections window shows that authentication has tailed for the user. The Mobility Controllers (MC's) RADIUS events show that it is receiving Access-Rejects for the authentication attempt.
What is one place that you can you look for deeper insight into why this authentication attempt is failing?
A. the reports generated by Aruba ClearPass Insight
B. the RADIUS events within the CPPM Event Viewer
C. the Alerts tab in the authentication record in CPPM Access Tracker
D. the packets captured on the MC control plane destined to UDP 1812
Answer: B (LEAVE A REPLY)
When an authentication attempt for a user's Windows domain computer is failing on a WPA3-Enterprise WLAN and the Mobility Controller is receiving Access-Rejects, one place to look for deeper insight is the RADIUS events within the CPPM Event Viewer. ClearPass Policy Manager (CPPM) logs all RADIUS authentication events, and the Event Viewer would show detailed information about why a particular authentication attempt was rejected. This could include reasons such as incorrect credentials, expired certificates, or policy mismatches. The CPPM Event Viewer is an essential troubleshooting tool within ClearPass to diagnose authentication issues, as indicated in the ClearPass Policy Manager documentation.

NEW QUESTION: 80

What is an example of passive endpoint classification?

A. TCP fingerprinting

B. SSH scans

C. WMI scans

D. SNMP scans

Answer: A (LEAVE A REPLY)

Endpoint classification in HPE Aruba Networking ClearPass Policy Manager (CPPM) involves identifying and categorizing devices on the network to enforce access policies. CPPM supports two types of profiling methods: passive and active.

Passive Profiling: Involves observing network traffic that devices send as part of their normal operation, without CPPM sending any requests to the device. Examples include DHCP fingerprinting, HTTP User-Agent analysis, and TCP fingerprinting.

Active Profiling: Involves CPPM sending requests to the device to gather information, such as SNMP scans, WMI scans, or SSH probes.

Option A, "TCP fingerprinting," is correct. TCP fingerprinting is a passive profiling method where CPPM analyzes TCP packet headers (e.g., TTL, window size) in the device's normal network traffic to identify its operating system. This does not require CPPM to send any requests to the device, making it a passive method.

Option B, "SSH scans," is incorrect. SSH scans involve actively connecting to a device over SSH to gather information (e.g., system details), which is an active profiling method.

Option C, "WMI scans," is incorrect. Windows Management Instrumentation (WMI) scans involve CPPM querying a Windows device to gather information (e.g., OS version, installed software), which is an active profiling method.

Option D, "SNMP scans," is incorrect. SNMP scans involve CPPM sending SNMP requests to a device to gather information (e.g., system description, interfaces), which is an active profiling method.

The HPE Aruba Networking ClearPass Policy Manager 6.11 User Guide states:

"Passive profiling methods observe network traffic that endpoints send as part of their normal operation, without ClearPass sending any requests to the device. An example of passive profiling is TCP fingerprinting, where ClearPass analyzes TCP packet headers (e.g., TTL, window size) to identify the device's operating system. Active profiling methods, such as SNMP scans, WMI scans, or SSH scans, involve ClearPass sending requests to the device to gather information." (Page 246, Passive vs. Active Profiling Section) Additionally, the ClearPass Device Insight Data Sheet notes:

"Passive profiling techniques, such as TCP fingerprinting, allow ClearPass to identify devices without generating additional network traffic. By analyzing TCP attributes in the device's normal traffic, ClearPass can fingerprint the OS, making it a non-intrusive method for endpoint classification." (Page 3, Profiling Methods Section)

:

HPE Aruba Networking ClearPass Policy Manager 6.11 User Guide, Passive vs. Active Profiling Section, Page 246.

ClearPass Device Insight Data Sheet, Profiling Methods Section, Page 3.

NEW QUESTION: 81
What is an example or phishing?
A. An attacker sends TCP messages to many different ports to discover which ports are open.
B. An attacker checks a user's password by using trying millions of potential passwords.
C. An attacker lures clients to connect to a software-based AP that is using a legitimate SSID.
D. An attacker sends emails posing as a service team member to get users to disclose their passwords.
Answer: D (LEAVE A REPLY)
Phishing is a type of social engineering attack where an attacker impersonates a trusted entity to deceive people into providing sensitive information, such as passwords or credit card numbers. An example of phishing is when an attacker sends emails posing as a service team member or a legitimate organization with the intention of getting users to disclose their passwords or other confidential information. These emails often contain links to fake websites that look remarkably similar to legitimate ones, tricking users into entering their details.References:
Cybersecurity guidelines on identifying and preventing phishing attacks.

NEW QUESTION: 82
Which is a correct description of a stage in the Lockheed Martin kill chain?
A. In the weaponization stage, which occurs after malware has been delivered to a system, the malware executes its function.
B. In the exploitation and installation phases, malware creates a backdoor into the infected system for the hacker.
C. In the reconnaissance stage, the hacker assesses the impact of the attack and how much information was exfiltrated.
D. In the delivery stage, malware collects valuable data and delivers or exfiltrates it to the hacker.
Answer: (SHOW ANSWER)
The Lockheed Martin Cyber Kill Chain is a framework that outlines the stages of a cyber attack, from initial reconnaissance to achieving the attacker's objective. It is often referenced in HPE Aruba Networking security documentation to help organizations understand and mitigate threats. The stages are: Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command and Control (C2), and Actions on Objectives.
Option A, "In the weaponization stage, which occurs after malware has been delivered to a system, the malware executes its function," is incorrect. The weaponization stage occurs before delivery, not after. In this stage, the attacker creates a deliverable payload (e.g., combining malware with an exploit). The execution of the malware happens in the exploitation stage, not weaponization.
Option B, "In the exploitation and installation phases, malware creates a backdoor into the infected system for the hacker," is correct. The exploitation phase involves the attacker exploiting a vulnerability (e.g., a software flaw) to execute the malware on the target system. The installation

phase follows, where the malware installs itself to establish persistence, often by creating a backdoor (e.g., a remote access tool) to allow the hacker to maintain access to the system. These two phases are often linked in the kill chain as the malware gains a foothold and ensures continued access.
Option C, "In the reconnaissance stage, the hacker assesses the impact of the attack and how much information was exfiltrated," is incorrect. The reconnaissance stage occurs at the beginning of the kill chain, where the attacker gathers information about the target (e.g., network topology, vulnerabilities). Assessing the impact and exfiltration occurs in the Actions on Objectives stage, the final stage of the kill chain.
Option D, "In the delivery stage, malware collects valuable data and delivers or exfiltrates it to the hacker," is incorrect. The delivery stage involves the attacker transmitting the weaponized payload to the target (e.g., via a phishing email). Data collection and exfiltration occur later, in the Actions on Objectives stage, not during delivery.
The HPE Aruba Networking Security Guide states:
"The Lockheed Martin Cyber Kill Chain outlines the stages of a cyber attack. In the exploitation phase, the attacker exploits a vulnerability to execute the malware on the target system. In the installation phase, the malware creates a backdoor or other persistence mechanism, such as a remote access tool, to allow the hacker to maintain access to the infected system for future actions." (Page 18, Cyber Kill Chain Overview Section) Additionally, the HPE Aruba Networking AOS-8 8.11 User Guide notes:
"The exploitation and installation phases of the Lockheed Martin kill chain involve the malware gaining a foothold on the target system. During exploitation, the malware is executed by exploiting a vulnerability, and during installation, it creates a backdoor to ensure persistent access for the hacker, enabling further stages like command and control." (Page 420, Threat Mitigation Section)
:
HPE Aruba Networking Security Guide, Cyber Kill Chain Overview Section, Page 18.
HPE Aruba Networking AOS-8 8.11 User Guide, Threat Mitigation Section, Page 420.

NEW QUESTION: 83
You have been instructed to look in the ArubaOS Security Dashboard's client list. Your goal is to find clients that belong to the company and have connected to devices that might belong to hackers.
Which client fits this description?
A. MAC address: d8:50:e6:f3:70:ab; Client Classification: Interfering; AP Classification: Rogue
B. MAC address: d8:50:e6:f3:6e:c5; Client Classification: Interfering; AP Classification: Neighbor
C. MAC address: d8:50:e6:f3:6e:60; Client Classification: Interfering; AP Classification: Authorized
D. MAC address: d8:50:e6:f3:6d:a4; Client Classification: Authorized; AP Classification: Rogue
Answer: D (LEAVE A REPLY)
The ArubaOS Security Dashboard, part of the AOS-8 architecture (Mobility Controllers or Mobility Master), provides visibility into wireless clients and access points (APs) through its Wireless

Intrusion Prevention (WIP) system. The goal is to identify clients that belong to the company (i.e., authorized clients) and have connected to devices that might belong to hackers (i.e., rogue APs).
Client Classification:
Authorized: A client that has successfully authenticated to an authorized AP and is recognized as part of the company's network (e.g., an employee device).
Interfering: A client that is not authenticated to the company's network and is considered external or potentially malicious.
AP Classification:
Authorized: An AP that is part of the company's network and managed by the MC/MM.
Rogue: An AP that is not authorized and is suspected of being malicious (e.g., connected to the company's wired network without permission).
Neighbor: An AP that is not part of the company's network but is not connected to the wired network (e.g., a nearby AP from another organization).
The requirement is to find a client that is authorized (belongs to the company) and connected to a rogue AP (might belong to hackers).
Option A: MAC address: d8:50:e6:f3:70:ab; Client Classification: Interfering; AP Classification: Rogue This client is classified as "Interfering," meaning it does not belong to the company. Although it is connected to a rogue AP, it does not meet the requirement of being a company client.
Option B: MAC address: d8:50:e6:f3:6e:c5; Client Classification: Interfering; AP Classification: Neighbor This client is "Interfering" (not a company client) and connected to a "Neighbor" AP, which is not considered a hacker's device (it's just a nearby AP).
Option C: MAC address: d8:50:e6:f3:6e:60; Client Classification: Interfering; AP Classification: Authorized This client is "Interfering" (not a company client) and connected to an "Authorized" AP, which is part of the company's network, not a hacker's device.
Option D: MAC address: d8:50:e6:f3:6d:a4; Client Classification: Authorized; AP Classification: Rogue This client is "Authorized," meaning it belongs to the company, and it is connected to a "Rogue" AP, which might belong to hackers. This matches the requirement perfectly.
The HPE Aruba Networking AOS-8 8.11 User Guide states:
"The Security Dashboard in ArubaOS provides a client list that includes the client classification and the AP classification for each client. A client classified as 'Authorized' has successfully authenticated to an authorized AP and is part of the company's network. A 'Rogue' AP is an unauthorized AP that is suspected of being malicious, often because it is connected to the company's wired network (e.g., detected via Eth-Wired-Mac-Table match). To identify potential security risks, look for authorized clients connected to rogue APs, as this may indicate that a company device has connected to a hacker's AP." (Page 415, Security Dashboard Section)
Additionally, the HPE Aruba Networking Security Guide notes:
"An 'Authorized' client is one that has authenticated to an AP managed by the controller, typically an employee or corporate device. A 'Rogue' AP is classified as such if it is not authorized and poses a potential threat, such as being connected to the corporate LAN. Identifying authorized

clients connected to rogue APs is critical for detecting potential man-in-the-middle attacks." (Page 78, WIP Classifications Section)
:
HPE Aruba Networking AOS-8 8.11 User Guide, Security Dashboard Section, Page 415.
HPE Aruba Networking Security Guide, WIP Classifications Section, Page 78.

NEW QUESTION: 84
A client has accessed an HTTPS server at myhost1.example.com using Chrome. The server sends a certificate that includes these properties:
Subject name: myhost.example.com
SAN: DNS: myhost.example.com; DNS: myhost1.example.com
Extended Key Usage (EKU): Server authentication
Issuer: MyCA_Signing
The server also sends an intermediate CA certificate for MyCA_Signing, which is signed by MyCA. The client's Trusted CA Certificate list does not include the MyCA or MyCA_Signing certificates.
Which factor or factors prevent the client from trusting the certificate?
A. The client does not have the correct trusted CA certificates.
B. The certificate lacks a valid SAN.
C. The certificate lacks the correct EKU.
D. The certificate lacks a valid SAN, and the client does not have the correct trusted CA certificates.
Answer: A (LEAVE A REPLY)
This question is identical to Question 17, with the same certificate properties and scenario. The client (Chrome browser) accesses an HTTPS server at myhost1.example.com, and the server presents a certificate with:
Subject name: myhost.example.com
SAN: DNS: myhost.example.com; DNS: myhost1.example.com
EKU: Server authentication
Issuer: MyCA_Signing (intermediate CA)
The intermediate CA certificate (MyCA_Signing) is signed by MyCA (root CA).
The client's Trusted CA Certificate list does not include MyCA or MyCA_Signing.
The certificate validation process is the same as in Question 17:
Name Validation: The SAN includes "myhost1.example.com," which matches the server's hostname, so this passes.
EKU Validation: The EKU is "Server authentication," which is correct for HTTPS, so this passes.
Chain of Trust Validation: The client attempts to build a chain from the server's certificate to a trusted root CA:
Server certificate → MyCA_Signing → MyCA Since MyCA is not in the client's Trusted CA Certificate list, the chain cannot be validated, and the client does not trust the certificate.

Option A, "The client does not have the correct trusted CA certificates," is correct. The absence of MyCA in the client's trust store prevents the client from validating the certificate chain.
Option B, "The certificate lacks a valid SAN," is incorrect because the SAN includes "myhost1.example.com," which is valid.
Option C, "The certificate lacks the correct EKU," is incorrect because the EKU is correctly set to "Server authentication." Option D, "The certificate lacks a valid SAN, and the client does not have the correct trusted CA certificates," is incorrect because the SAN is valid; the only issue is the missing trusted CA certificates.
The HPE Aruba Networking AOS-CX 10.12 Security Guide states:
"For a client to trust a server's certificate during HTTPS communication, the client must validate the certificate chain to a trusted root CA in its trust store. If the root CA (e.g., MyCA) or intermediate CA (e.g., MyCA_Signing) is not in the client's Trusted CA Certificate list, the chain of trust cannot be established, and the client will reject the certificate. The Subject Alternative Name (SAN) must include the server's hostname, and the Extended Key Usage (EKU) must include 'Server authentication' for HTTPS." (Page 205, Certificate Validation Section) Additionally, the HPE Aruba Networking Security Fundamentals Guide notes:
"A common reason for certificate validation failure is the absence of the root CA certificate in the client's trust store. For example, if a server's certificate is issued by an intermediate CA (e.g., MyCA_Signing) that chains to a root CA (e.g., MyCA), the client must have the root CA certificate in its Trusted CA Certificate list to trust the chain." (Page 45, Certificate Trust Issues Section)
:
HPE Aruba Networking AOS-CX 10.12 Security Guide, Certificate Validation Section, Page 205.
HPE Aruba Networking Security Fundamentals Guide, Certificate Trust Issues Section, Page 45.

NEW QUESTION: 85
What is an Authorized client as defined by ArubaOS Wireless Intrusion Prevention System (WIP)?
A. a client that has a certificate issued by a trusted Certification Authority (CA)
B. a client that is not on the WIP blacklist
C. a client that has successfully authenticated to an authorized AP and passed encrypted traffic
D. a client that is on the WIP whitelist.
Answer: C (LEAVE A REPLY)
In the context of ArubaOS Wireless Intrusion Prevention System (WIP), an authorized client is defined as a client that has successfully authenticated to an authorized Access Point (AP) and has passed encrypted traffic.
This ensures that only clients which have been verified and authenticated according to the network's security policies are allowed to access network resources. Authentication typically involves credentials that are validated by a server, confirming the client's right to access the network securely.References:
ArubaOS Wireless Intrusion Prevention System configuration and management guidelines.

NEW QUESTION: 86
What is a correct guideline for the management protocols that you should use on ArubaOS-Switches?
A. Disable Telnet and use TFTP instead.
B. Disable SSH and use https instead.
C. Disable Telnet and use SSH instead
D. Disable HTTPS and use SSH instead
Answer: C (LEAVE A REPLY)
In managing ArubaOS-Switches, the best practice is to disable less secure protocols such as Telnet and use more secure alternatives like SSH (Secure Shell). SSH provides encrypted connections between network devices, which is critical for maintaining the security and integrity of network communications. This guideline is aligned with general security best practices that prioritize the use of protocols with strong, built-in encryption mechanisms to prevent unauthorized access and ensure data privacy.

NEW QUESTION: 87
What does the NIST model for digital forensics define?
A. how to define access control policies that will properly protect a company's most sensitive data and digital resources
B. how to properly collect, examine, and analyze logs and other data, in order to use it as evidence in a security investigation
C. which types of architecture and security policies are best equipped to help companies establish a Zero Trust Network (ZTN)
D. which data encryption and authentication algorithms are suitable for enterprise networks in a world that is moving toward quantum computing
Answer: B (LEAVE A REPLY)
The National Institute of Standards and Technology (NIST) provides guidelines on digital forensics, which include methodologies for properly collecting, examining, and analyzing digital evidence. This framework helps ensure that digital evidence is handled in a manner that preserves its integrity and maintains its admissibility in legal proceedings:
Digital Forensics Process: This process involves steps to ensure that data collected from digital sources can be used reliably in investigations and court cases, addressing chain-of-custody issues, proper evidence handling, and detailed documentation of forensic procedures.

NEW QUESTION: 88
What is symmetric encryption?
A. It simultaneously creates ciphertext and a same-size MAC.
B. It any form of encryption mat ensures that thee ciphertext Is the same length as the plaintext.
C. It uses the same key to encrypt plaintext as to decrypt ciphertext.
D. It uses a Key that is double the size of the message which it encrypts.
Answer: C (LEAVE A REPLY)

Symmetric encryption is a type of encryption where the same key is used to encrypt and decrypt the message. It's called "symmetric" because the key used for encryption is identical to the key used for decryption. The data, or plaintext, is transformed into ciphertext during encryption, and then the same key is used to revert the ciphertext back to plaintext during decryption. It is a straightforward method but requires secure handling and exchange of the encryption key.
:
Basic principles of cryptography.

NEW QUESTION: 89
You have been asked to send RADIUS debug messages from an AOS-CX switch to a central SIEM server at 10.5.15.6. The server is already defined on the switch with this command:
logging 10.5.15.6
You enter this command:
debug radius all
What is the correct debug destination?
A. file
B. console
C. buffer
D. syslog
Answer: D (LEAVE A REPLY)
The scenario involves an AOS-CX switch that needs to send RADIUS debug messages to a central SIEM server at 10.5.15.6. The switch has already been configured to send logs to the SIEM server with the command logging 10.5.15.6, and the command debug radius all has been entered to enable RADIUS debugging.
Debug Command: The debug radius all command enables debugging for all RADIUS-related events on the AOS-CX switch, generating detailed debug messages for RADIUS authentication, accounting, and other operations.
Debug Destination: Debug messages on AOS-CX switches can be sent to various destinations, such as the console, a file, the debug buffer, or a Syslog server. The logging 10.5.15.6 command indicates that the switch is configured to send logs to a Syslog server at 10.5.15.6 (using UDP port 514 by default, unless specified otherwise).
Option D, "syslog," is correct. To send RADIUS debug messages to the SIEM server, the debug destination must be set to "syslog," as the SIEM server is already defined as a Syslog destination with logging 10.5.15.6. The command to set the debug destination to Syslog is debug destination syslog, which ensures that the RADIUS debug messages are sent to the configured Syslog server (10.5.15.6).
Option A, "file," is incorrect. Sending debug messages to a file (e.g., using debug destination file) stores the messages on the switch's filesystem, not on the SIEM server.
Option B, "console," is incorrect. Sending debug messages to the console (e.g., using debug destination console) displays them on the switch's console session, not on the SIEM server.

Option C, "buffer," is incorrect. Sending debug messages to the buffer (e.g., using debug destination buffer) stores them in the switch's debug buffer, which can be viewed with show debug buffer, but does not send them to the SIEM server.
The HPE Aruba Networking AOS-CX 10.12 System Management Guide states:
"To send debug messages, such as RADIUS debug messages, to a central SIEM server, first configure the Syslog server with the logging <ip-address> command (e.g., logging 10.5.15.6). Then, enable the desired debug with a command like debug radius all, and set the debug destination to Syslog using debug destination syslog. This ensures that all debug messages are sent to the configured Syslog server for centralized logging." (Page 92, Debug Logging Section)
Additionally, the HPE Aruba Networking AOS-CX 10.12 Security Guide notes:
"RADIUS debug messages can be sent to a Syslog server for centralized monitoring. After enabling RADIUS debugging with debug radius all, use debug destination syslog to send the messages to the Syslog server configured with the logging command, such as a SIEM server at 10.5.15.6." (Page 152, RADIUS Debugging Section)
:
HPE Aruba Networking AOS-CX 10.12 System Management Guide, Debug Logging Section, Page 92.
HPE Aruba Networking AOS-CX 10.12 Security Guide, RADIUS Debugging Section, Page 152.

NEW QUESTION: 90
Your Aruba Mobility Master-based solution has detected a rogue AP Among other information the ArubaOS Detected Radios page lists this Information for the AP SSID = PubllcWiFI BSSID = a8M27 12 34:56 Match method = Exact match Match type = Eth-GW-wired-Mac-Table The security team asks you to explain why this AP is classified as a rogue. What should you explain?
A. The AP Is connected to your LAN because It is transmitting wireless traffic with your network's default gateway's MAC address as a source MAC Because it does not belong to the company, it is a rogue
B. The AP has been detected as launching a DoS attack against your company's default gateway. This qualities it as a rogue which needs to be contained with wireless association frames immediately
C. The ap has a BSSID mat matches authorized client MAC addresses. This indicates that the AP is spoofing the MAC address to gam unauthorized access to your company's wireless services, so It is a rogue
D. The AP is spoofing a routers MAC address as its BSSID. This indicates mat, even though WIP cannot determine whether the AP is connected to your LAN. it is a rogue.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 91
Which correctly describes a way to deploy certificates to end-user devices?
A. ClearPass Onboard can help to deploy certificates to end-user devices, whether or not they are members of a Windows domain

B. ClearPass Device Insight can automatically discover end-user devices and deploy the proper certificates to them
C. ClearPass OnGuard can help to deploy certificates to end-user devices, whether or not they are members of a Windows domain
D. in a Windows domain, domain group policy objects (GPOs) can automatically install computer, but not user certificates
Answer: A (LEAVE A REPLY)
ClearPass Onboard is part of the Aruba ClearPass suite and it provides a mechanism to deploy certificates to end-user devices, regardless of whether or not they are members of a Windows domain. ClearPass Onboard facilitates the configuration and provisioning of network settings and security, including the delivery and installation of certificates to ensure secure network access. This capability enables a bring-your-own-device (BYOD) environment where devices can be securely managed and provided with the necessary certificates for network authentication.

NEW QUESTION: 92
You are managing an Aruba Mobility Controller (MC). What is a reason for adding a "Log Settings" definition in the ArubaOS Diagnostics > System > Log Settings page?
A. Configuring the Syslog server settings for the server to which the MC forwards logs for a particular category and level
B. Configuring the MC to generate logs for a particular event category and level, but only for a specific user or AP.
C. Configuring a filter that you can apply to a defined Syslog server in order to filter events by subcategory
D. Configuring the log facility and log format that the MC will use for forwarding logs to all Syslog servers
Answer: A (LEAVE A REPLY)
The primary reason for adding a "Log Settings" definition in the ArubaOS Diagnostics > System > Log Settings page is to configure the Syslog server settings for the server to which the Mobility Controller (MC) forwards logs for a particular category and level. This setting enables the MC to send detailed logs to a Syslog server for centralized logging and monitoring, which is essential for troubleshooting, security analysis, and compliance with various policies.References:
ArubaOS documentation on log management and Syslog configuration.

NEW QUESTION: 93
What is a benefit of deploying Aruba ClearPass Device insight?
A. visibility into devices' 802.1X supplicant settings and automated certificate deployment
B. Simpler troubleshooting of ClearPass solutions across an environment with multiple ClearPass Policy Managers
C. Agent-based analysts of devices' security settings and health status, with the ability to implement quarantining
D. Highly accurate endpoint classification for environments with many devices types, including Internet of Things (IoT)
Answer: A (LEAVE A REPLY)

NEW QUESTION: 94
Refer to the exhibit, which shows the settings on the company's MCs.
- Mobility Controller
Dashboard General Admin AirWave CPSec Certificates
Configuration
WLANs v Control Plane Security
Roles & Policies Enable CP Sec
Access Points Enable auto cert provisioning:
You have deployed about 100 new Aruba 335-APs. What is required for the APs to become managed?
A. installing CA-signed certificates on the APs
B. installing self-signed certificates on the APs
C. approving the APs as authorized APs on the AP whitelist
D. configuring a PAPI key that matches on the APs and MCs
Answer: C (LEAVE A REPLY)
Based on the exhibit, which shows the settings on the company's Mobility Controllers (MCs), with 'Control Plane Security' enabled and 'Enable auto cert provisioning' available, new Aruba 335-APs require approval on the MC to become managed. This is commonly done by adding the APs to an authorized AP whitelist, after which they can be automatically provisioned with certificates generated by the MC.

NEW QUESTION: 95
Your Aruba Mobility Master-based solution has detected a rogue AP Among other information the ArubaOS Detected Radios page lists this Information for the AP SSID = PubllcWiFI BSSID = a8M27 12 34:56 Match method = Exact match Match type = Eth-GW-wired-Mac-Table The security team asks you to explain why this AP is classified as a rogue. What should you explain?
A. The AP Is connected to your LAN because It is transmitting wireless traffic with your network's default gateway's MAC address as a source MAC Because it does not belong to the company, it is a rogue

B. The ap has a BSSID mat matches authorized client MAC addresses. This indicates that the AP is spoofing the MAC address to gam unauthorized access to your company's wireless services, so It is a rogue
C. The AP has been detected as launching a DoS attack against your company's default gateway. This qualities it as a rogue which needs to be contained with wireless association frames immediately
D. The AP is spoofing a routers MAC address as its BSSID. This indicates mat, even though WIP cannot determine whether the AP is connected to your LAN. it is a rogue.
Answer: A (LEAVE A REPLY)
The AP is classified as a rogue because it is connected to your LAN and is transmitting wireless traffic with your network's default gateway's MAC address as a source MAC. In this scenario, the 'Match method = Exact match' and 'Match type = Eth-GW-wired-Mac-Table' indicates that the rogue AP has been detected by matching the Ethernet gateway's MAC address, which is on the wired network, implying that the rogue AP is connected to the corporate LAN. Since the AP does not belong to the company, its presence on the network is unauthorized and is thus classified as a rogue AP.
:
ArubaOS documentation on rogue AP detection and classification.
Wireless security best practices that explain how the presence of unauthorized APs on the LAN constitutes a security threat.

NEW QUESTION: 96
What are the roles of 802.1X authenticators and authentication servers?
A. The authenticator stores the user account database, while the server stores access policies.
B. The authenticator supports only EAP, while the authentication server supports only RADIUS.
C. The authenticator is a RADIUS client and the authentication server is a RADIUS server.
D. The authenticator makes access decisions and the server communicates them to the supplicant.
Answer: C (LEAVE A REPLY)
In the 802.1X network access control model, the roles of the authenticator and the authentication server are distinct yet complementary. The authenticator acts as a RADIUS client, which is a network device, like a switch or wireless access point, that directly interfaces with the client machine (supplicant). The authentication server, typically a RADIUS server, is responsible for verifying the credentials provided by the supplicant through the authenticator. This setup helps in separating the duties where the authenticator enforces authentication but does not decide on the validity of the credentials, which is the role of the authentication server.
:
IEEE 802.1X standard for network access control.

NEW QUESTION: 97

A company has Aruba Mobility Controllers (MCs). Aruba campus APs. and ArubaOS-CX switches. The company plans to use ClearPass Policy Manager (CPPM) to classify endpoints by type The ClearPass admins tell you that they want to run Network scans as part of the solution What should you do to configure the infrastructure to support the scans?

A. Create a TA profile on the ArubaOS-Switches with the root CA certificate for ClearPass's HTTPS certificate

B. Create device fingerprinting profiles on the ArubaOS-Switches that include SNMP. and apply the profiles to edge ports

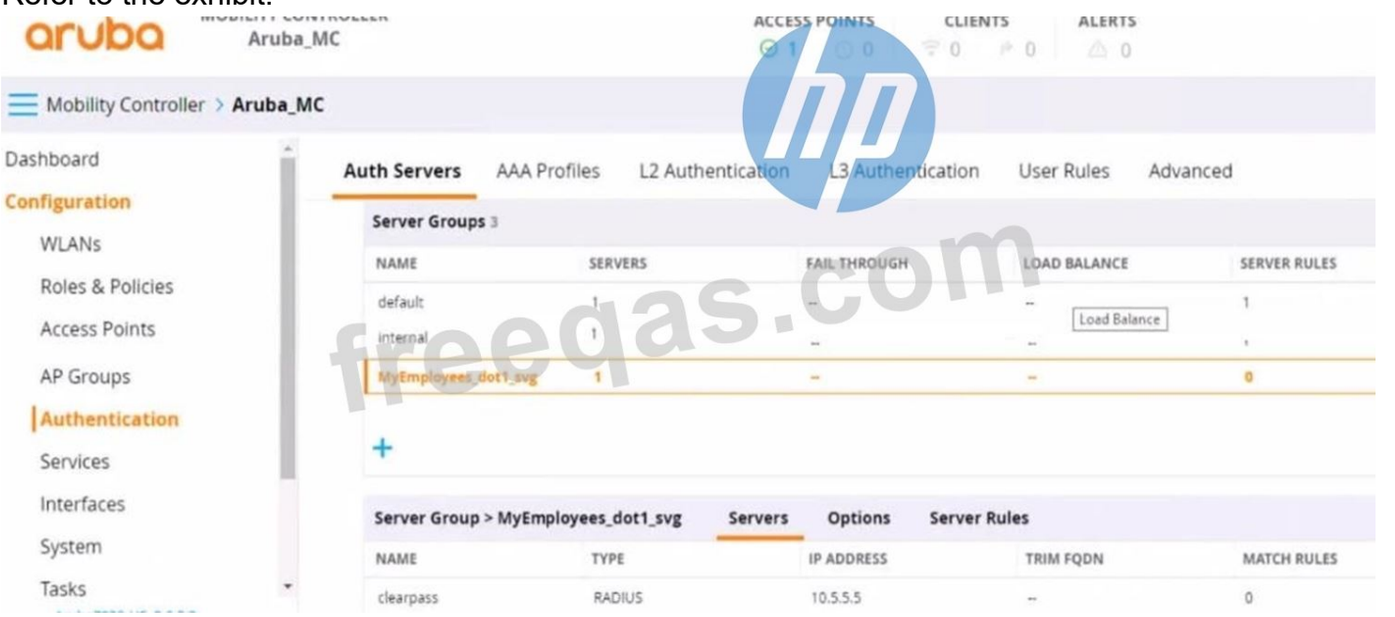
C. Create SNMPv3 users on ArubaOS-CX switches, and make sure that the credentials match those configured on CPPM

D. Create remote mirrors on the ArubaOS-Swrtches that collect traffic on edge ports, and mirror it to CPPM's IP address.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 98

Refer to the exhibit.



You have set up a RADIUS server on an ArubaOS Mobility Controller (MC) when you created a WLAN named "MyEmployees .You now want to enable the MC to accept change of authorization (CoA) messages from this server for wireless sessions on this WLAN.

What Is a part of the setup on the MC?

A. Create a dynamic authorization, or RFC 3576, server with the 10.5.5.5 address and correct shared secret.

B. Install the root CA associated with the 10 5.5.5 server's certificate as a Trusted CA certificate.

C. Configure a ClearPass username and password in the MyEmployees AAA profile.

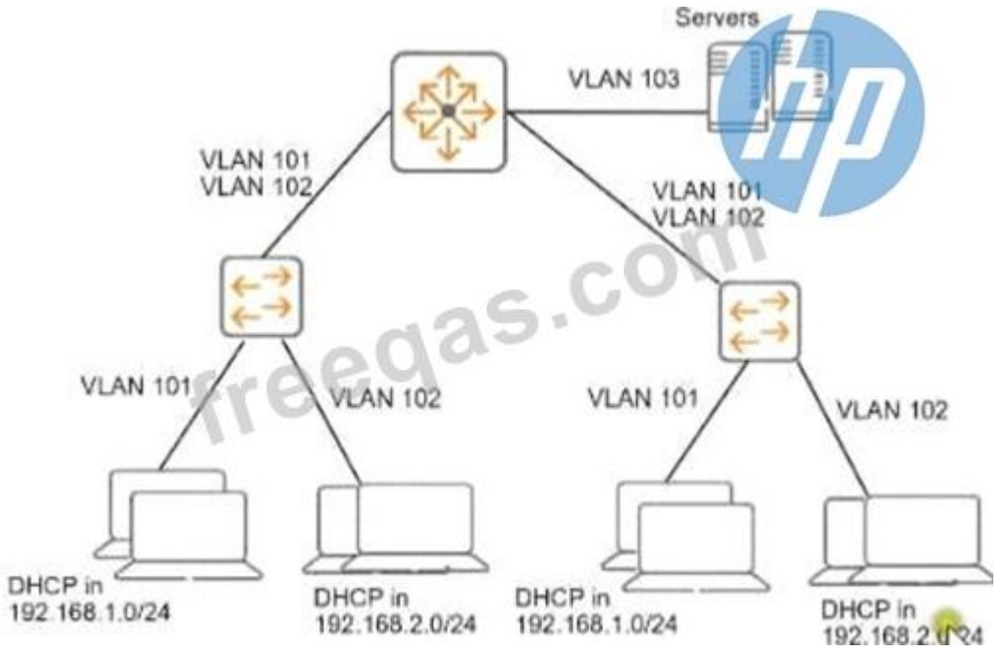
D. Enable the dynamic authorization setting in the "clearpass" authentication server settings.

Answer: A (LEAVE A REPLY)

To enable an ArubaOS Mobility Controller (MC) to accept Change of Authorization (CoA) messages from a RADIUS server for wireless sessions on a WLAN, part of the setup on the MC

involves creating a dynamic authorization, or RFC 3576, server with the provided IP address (10.5.5.5) and the correct shared secret. This setup allows the MC to handle CoA requests, which are used to change the authorization attributes of a session after it has been authenticated, such as disconnecting a user or changing a user's VLAN assignment.

NEW QUESTION: 99
Refer to the exhibit.



You need to ensure that only management stations in subnet 192.168.1.0/24 can access the ArubaOS-Switches' CLI. Web UI. and REST interfaces The company also wants to let managers use these stations to access other parts of the network What should you do?
A. Establish a Control Plane Policing class that selects traffic from 192.168 1.0/24.
B. Specify 192.168.1.0.255.255.255.0 as authorized IP manager address
C. Configure the switch to listen for these protocols on OOBM only.
D. Specify vlan 100 as the management vlan for the switches.
Answer: (SHOW ANSWER)
To ensure that only management stations in the subnet 192.168.1.0/24 can access the ArubaOS-Switches' Command Line Interface (CLI), Web UI, and REST interfaces, while also allowing managers to access other parts of the network, you should specify 192.168.1.0 255.255.255.0 as the authorized manager IP address on the switches. This configuration will restrict access to the switch management interfaces to devices within the specified IP address range, effectively creating a management access list.
References:
ArubaOS-Switch management and configuration guide detailing IP authorized manager settings.
Network management best practices which recommend controlling access to network devices' management interfaces.

NEW QUESTION: 100

What is a benefit of Protected Management Frames (PMF). sometimes called Management Frame Protection (MFP)?
A. PMF helps to protect APs and MCs from unauthorized management access by hackers.
B. PMF ensures trial traffic between APs and Mobility Controllers (MCs) is encrypted.
C. PMF prevents hackers from capturing the traffic between APs and Mobility Controllers.
D. PMF protects clients from DoS attacks based on forged de-authentication frames
Answer: (SHOW ANSWER)
Protected Management Frames (PMF), also known as Management Frame Protection (MFP), is designed to protect clients from denial-of-service (DoS) attacks that involve forged de-authentication and disassociation frames. These attacks can disconnect legitimate clients from the network. PMF provides a way to authenticate these management frames, ensuring that they are not forged, thus enhancing the security of the wireless network.
:
IEEE 802.11w amendment, which introduces PMF as a security enhancement to protect management frames.
Wi-Fi Alliance security guidelines for Protected Management Frames (PMF).

NEW QUESTION: 101
Which is a correct description of a stage in the Lockheed Martin kill chain?
A. In the exploitation and installation phases, malware creates a backdoor into the infected system for the hacker.
B. In the reconnaissance stage, the hacker assesses the impact of the attack and how much information was exfilltrated.
C. In the delivery stage, malware collects valuable data and delivers or exfilltrated it to the hacker.
D. In the weaponization stage, which occurs after malware has been delivered to a system, the malware executes Its function.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 102
You have configured a WLAN to use Enterprise security with the WPA3 version.
How does the WLAN handle encryption?
A. Traffic is encrypted with TKIP and keys derived from a PMK shared by all clients on the WLAN.
B. Traffic is encrypted with TKIP and keys derived from a unique PMK per client.
C. Traffic is encrypted with AES and keys derived from a PMK shared by all clients on the WLAN.
D. Traffic is encrypted with AES and keys derived from a unique PMK per client.
Answer: (SHOW ANSWER)
WPA3-Enterprise is a security protocol introduced to enhance the security of wireless networks, particularly in enterprise environments. It builds on the foundation of WPA2 but introduces stronger encryption and key management practices. In WPA3-Enterprise, authentication is typically performed using 802.1X, and encryption is handled using the Advanced Encryption Standard (AES).

WPA3-Enterprise Encryption: WPA3-Enterprise uses AES with the Galois/Counter Mode Protocol (GCMP) or Cipher Block Chaining Message Authentication Code Protocol (CCMP), both of which are AES-based encryption methods. WPA3 does not use TKIP (Temporal Key Integrity Protocol), which is a legacy encryption method used in WPA and early WPA2 deployments and is considered insecure.
Pairwise Master Key (PMK): In WPA3-Enterprise, the PMK is derived during the 802.1X authentication process (e.g., via EAP-TLS or EAP-TTLS). Each client authenticates individually with the authentication server (e.g., ClearPass), resulting in a unique PMK for each client. This PMK is then used to derive session keys (Pairwise Transient Keys, PTKs) for encrypting the client's traffic, ensuring that each client's traffic is encrypted with unique keys.
Option A, "Traffic is encrypted with TKIP and keys derived from a PMK shared by all clients on the WLAN," is incorrect because WPA3 does not use TKIP (it uses AES), and the PMK is not shared among clients in WPA3-Enterprise; each client has a unique PMK.
Option B, "Traffic is encrypted with TKIP and keys derived from a unique PMK per client," is incorrect because WPA3 does not use TKIP; it uses AES.
Option C, "Traffic is encrypted with AES and keys derived from a PMK shared by all clients on the WLAN," is incorrect because, in WPA3-Enterprise, the PMK is unique per client, not shared.
Option D, "Traffic is encrypted with AES and keys derived from a unique PMK per client," is correct. WPA3-Enterprise uses AES for encryption, and each client derives a unique PMK during 802.1X authentication, which is used to generate unique session keys for encryption.
The HPE Aruba Networking AOS-8 8.11 User Guide states:
"WPA3-Enterprise enhances security by using AES encryption with GCMP or CCMP. In WPA3-Enterprise mode, each client authenticates via 802.1X, resulting in a unique Pairwise Master Key (PMK) for each client. The PMK is used to derive session keys (Pairwise Transient Keys, PTKs) that encrypt the client's traffic with AES, ensuring that each client's traffic is protected with unique keys. WPA3 does not support TKIP, which is a legacy encryption method." (Page 285, WPA3-Enterprise Security Section) Additionally, the HPE Aruba Networking Wireless Security Guide notes:
"WPA3-Enterprise requires 802.1X authentication, which generates a unique PMK for each client. This PMK is used to derive AES-based session keys, providing individualized encryption for each client's traffic and eliminating the risks associated with shared keys." (Page 32, WPA3 Security Features Section)
:
HPE Aruba Networking AOS-8 8.11 User Guide, WPA3-Enterprise Security Section, Page 285.
HPE Aruba Networking Wireless Security Guide, WPA3 Security Features Section, Page 32.

NEW QUESTION: 103
How can hackers implement a man-in-the-middle (MITM) attack against a wireless client?
A. The hacker uses a combination of software and hardware to jam the RF band and prevent the client from connecting to any wireless networks.

B. The hacker runs an NMap scan on the wireless client to find its MAC and IP address. The hacker then connects to another network and spoofs those addresses.
C. The hacker uses spear-phishing to probe for the IP addresses that the client is attempting to reach. The hacker device then spoofs those IP addresses.
D. The hacker connects a device to the same wireless network as the client and responds to the client's ARP requests with the hacker device's MAC address.
Answer: D (LEAVE A REPLY)
A man-in-the-middle (MITM) attack involves an attacker positioning themselves between a wireless client and the legitimate network to intercept or manipulate traffic. HPE Aruba Networking documentation often discusses MITM attacks in the context of wireless security threats and mitigation strategies.
Option D, "The hacker connects a device to the same wireless network as the client and responds to the client's ARP requests with the hacker device's MAC address," is correct. This describes an ARP poisoning (or ARP spoofing) attack, a common MITM technique in wireless networks. The hacker joins the same wireless network as the client (e.g., by authenticating with the same SSID and credentials). Once on the network, the hacker sends fake ARP responses to the client, associating the hacker's MAC address with the IP address of the default gateway (or another target device). This causes the client to send traffic to the hacker's device instead of the legitimate gateway, allowing the hacker to intercept, modify, or forward the traffic, thus performing an MITM attack.
Option A, "The hacker uses a combination of software and hardware to jam the RF band and prevent the client from connecting to any wireless networks," is incorrect. Jamming the RF band would disrupt all wireless communication, including the hacker's ability to intercept traffic. This is a denial-of-service (DoS) attack, not an MITM attack.
Option B, "The hacker runs an NMap scan on the wireless client to find its MAC and IP address. The hacker then connects to another network and spoofs those addresses," is incorrect. NMap scans are used for network discovery and port scanning, not for implementing an MITM attack. Spoofing MAC and IP addresses on another network does not position the hacker to intercept the client's traffic on the original network.
Option C, "The hacker uses spear-phishing to probe for the IP addresses that the client is attempting to reach. The hacker device then spoofs those IP addresses," is incorrect. Spear-phishing is a delivery method for malware or credentials theft, not a direct method for implementing an MITM attack. Spoofing IP addresses alone does not allow the hacker to intercept traffic unless they are on the same network and can manipulate routing (e.g., via ARP poisoning).
The HPE Aruba Networking AOS-8 8.11 User Guide states:
"A common man-in-the-middle (MITM) attack against wireless clients involves ARP poisoning. The hacker connects a device to the same wireless network as the client and sends fake ARP responses to the client, associating the hacker's MAC address with the IP address of the default gateway. This causes the client to send traffic to the hacker's device, allowing the hacker to

intercept and manipulate the traffic." (Page 422, Wireless Threats Section) Additionally, the HPE Aruba Networking Security Guide notes:
"ARP poisoning is a prevalent MITM attack in wireless networks. The attacker joins the same network as the client and responds to the client's ARP requests with the attacker's MAC address, redirecting traffic through the attacker's device. This allows the attacker to intercept sensitive data or modify traffic between the client and the legitimate destination." (Page 72, Wireless MITM Attacks Section)
:
HPE Aruba Networking AOS-8 8.11 User Guide, Wireless Threats Section, Page 422.
HPE Aruba Networking Security Guide, Wireless MITM Attacks Section, Page 72.

NEW QUESTION: 104
You are deploying a new wireless solution with an Aruba Mobility Master (MM). Aruba Mobility Controllers (MCs), and campus APs (CAPs). The solution will include a WLAN that uses Tunnel for the forwarding mode and WPA3-Enterprise for the security option.
You have decided to assign the WLAN to VLAN 301, a new VLAN. A pair of core routing switches will act as the default router for wireless user traffic.
Which links need to carry VLAN 301?
A. only links in the campus LAN to ensure seamless roaming
B. only links between MC ports and the core routing switches
C. only links on the path between APs and the core routing switches
D. only links on the path between APs and the MC
Answer: (SHOW ANSWER)
In a wireless network deployment with Aruba Mobility Master (MM), Mobility Controllers (MCs), and Campus APs (CAPs), where a WLAN is configured to use Tunnel mode for forwarding, the user traffic is tunneled from the APs to the MCs. VLAN 301, which is assigned to the WLAN, must be present on the links from the MCs to the core routing switches because these switches act as the default router for the wireless user traffic. It is not necessary for the VLAN to be present on all campus LAN links or AP links, only between the MCs and the core routing switches where the routing for VLAN 301 will occur.

NEW QUESTION: 105
What is a benefit of Protected Management Frames (PMF). sometimes called Management Frame Protection (MFP)?
A. PMF helps to protect APs and MCs from unauthorized management access by hackers.
B. PMF ensures trial traffic between APs and Mobility Controllers (MCs) is encrypted.
C. PMF prevents hackers from capturing the traffic between APs and Mobility Controllers.
D. PMF protects clients from DoS attacks based on forged de-authentication frames
Answer: D (LEAVE A REPLY)
Protected Management Frames (PMF), also known as Management Frame Protection (MFP), is designed to protect clients from denial-of-service (DoS) attacks that involve forged de-

authentication and disassociation frames. These attacks can disconnect legitimate clients from the network. PMF provides a way to authenticate these management frames, ensuring that they are not forged, thus enhancing the security of the wireless network.
References:
IEEE 802.11w amendment, which introduces PMF as a security enhancement to protect management frames.
Wi-Fi Alliance security guidelines for Protected Management Frames (PMF).

NEW QUESTION: 106
Refer to the exhibit.
You are deploying a new HPE Aruba Networking Mobility Controller (MC), which is enforcing authentication to HPE Aruba Networking ClearPass Policy Manager (CPPM). The authentication is not working correctly, and you find the error shown in the exhibit in the CPPM Event Viewer.
What should you check?
A. That the IP address that the MC is using to reach CPPM matches the one defined for the device on CPPM
B. That the MC has valid admin credentials configured on it for logging into the CPPM
C. That the MC has been added as a domain machine on the Active Directory domain with which CPPM is synchronized
D. That the shared secret configured for the CPPM authentication server matches the one defined for the device on CPPM
Answer: A (LEAVE A REPLY)
The exhibit shows an error in the CPPM Event Viewer: "RADIUS authentication attempt from unknown NAD 10.1.10.8:1812." This indicates that a new HPE Aruba Networking Mobility Controller (MC) is attempting to send RADIUS authentication requests to HPE Aruba Networking ClearPass Policy Manager (CPPM), but CPPM does not recognize the MC as a Network Access Device (NAD), resulting in the authentication failure.
Unknown NAD Error: In CPPM, a NAD is a device (e.g., an MC, switch, or AP) that sends RADIUS requests to CPPM for authentication. Each NAD must be configured in CPPM with its IP address and a shared secret. The error "unknown NAD 10.1.10.8:1812" means that the IP address 10.1.10.8 (the source IP of the MC's RADIUS request) is not listed as a NAD in CPPM's configuration, so CPPM rejects the request.
Option A, "That the IP address that the MC is using to reach CPPM matches the one defined for the device on CPPM," is correct. You need to check that the MC's IP address (10.1.10.8) is correctly configured as a NAD in CPPM. In CPPM, go to Configuration > Network > Devices, and verify that a NAD entry exists for 10.1.10.8. If the IP address does not match (e.g., due to NAT, a different interface, or a misconfiguration), CPPM will reject the request as coming from an unknown NAD.
Option B, "That the MC has valid admin credentials configured on it for logging into the CPPM," is incorrect. Admin credentials on the MC are used for management access (e.g., SSH, web UI), not

for RADIUS authentication. RADIUS communication between the MC and CPPM uses a shared secret, not admin credentials.
Option C, "That the MC has been added as a domain machine on the Active Directory domain with which CPPM is synchronized," is incorrect. Adding the MC as a domain machine in Active Directory (AD) is relevant only if the MC itself is authenticating users against AD (e.g., for machine authentication), but this is not required for the MC to act as a NAD sending RADIUS requests to CPPM.
Option D, "That the shared secret configured for the CPPM authentication server matches the one defined for the device on CPPM," is incorrect in this context. While a shared secret mismatch would cause authentication failures, it would not result in an "unknown NAD" error. The "unknown NAD" error occurs before the shared secret is checked, as CPPM does not recognize the IP address as a valid NAD.
The HPE Aruba Networking ClearPass Policy Manager 6.11 User Guide states:
"The error 'RADIUS authentication attempt from unknown NAD <IP-address>' in the Event Viewer indicates that the IP address of the device sending the RADIUS request (e.g., a Mobility Controller) is not configured as a Network Access Device (NAD) in ClearPass. To resolve this, go to Configuration > Network > Devices in the CPPM UI, and ensure that the IP address of the device (e.g., 10.1.10.8) is added as a NAD with the correct shared secret. The IP address used by the device to reach CPPM must match the one defined in the NAD configuration." (Page 302, Troubleshooting RADIUS Issues Section) Additionally, the HPE Aruba Networking AOS-8 8.11 User Guide notes:
"When configuring a Mobility Controller to use ClearPass as a RADIUS server, ensure that the MC's IP address is added as a NAD in ClearPass. If ClearPass logs an 'unknown NAD' error, verify that the IP address the MC uses to send RADIUS requests (e.g., the source IP of the request) matches the IP address configured in ClearPass under Configuration > Network > Devices." (Page 498, Configuring RADIUS Authentication Section)
:
HPE Aruba Networking ClearPass Policy Manager 6.11 User Guide, Troubleshooting RADIUS Issues Section, Page 302.
HPE Aruba Networking AOS-8 8.11 User Guide, Configuring RADIUS Authentication Section, Page 498.

NEW QUESTION: 107
Why might devices use a Diffie-Hellman exchange?
A. to agree on a shared secret in a secure manner over an insecure network
B. to obtain a digital certificate signed by a trusted Certification Authority
C. to prove knowledge of a passphrase without transmitting the passphrase
D. to signal that they want to use asymmetric encryption for future communications
Answer: A (LEAVE A REPLY)
Devices use the Diffie-Hellman exchange to agree on a shared secret in a secure manner over an insecure network. The main purpose of this cryptographic protocol is to enable two parties to establish a shared secret over an unsecured communication channel. This shared secret can then be used to encrypt subsequent communications using a symmetric key cipher. The Diffie-Hellman exchange is particularly valuable because it allows the secure exchange of cryptographic keys over a public channel without the need for a prior shared secret. This protocol is a foundational element for many secure communications protocols, including SSL/TLS, which is used to secure connections on the internet. References to the Diffie-Hellman protocol and its uses can be found in standard cryptographic textbooks and documentation such as those from the Internet Engineering Task Force (IETF) and security protocol specifications.