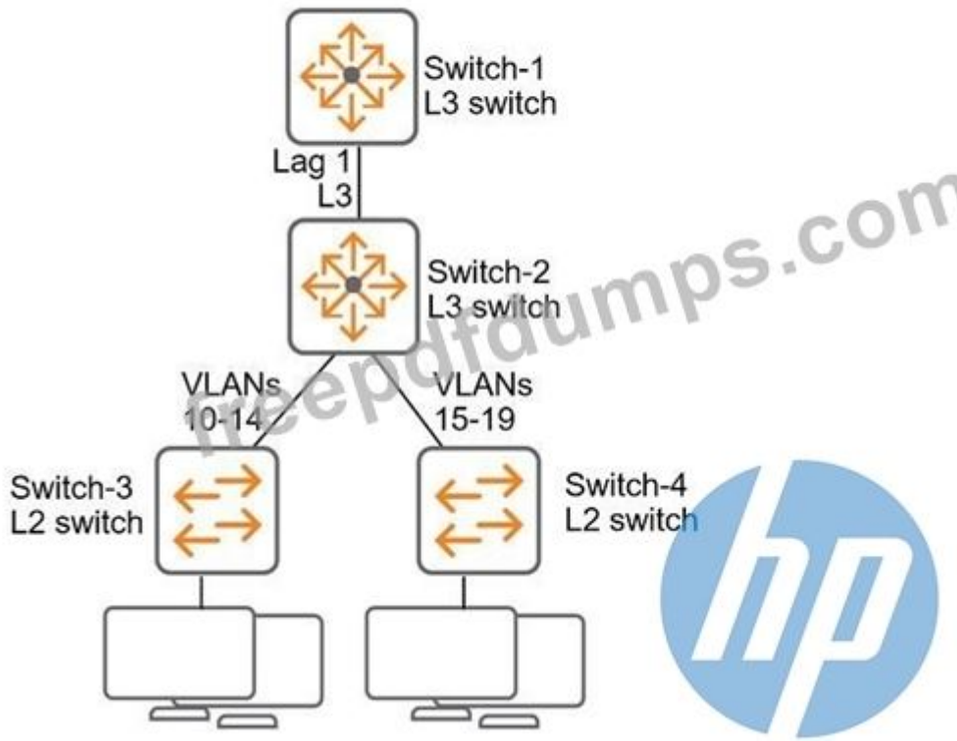
HP.HPE7-A02.v2025-07-15.q62

Exam Code:	HPE7-A02
Exam Name:	Aruba Certified Network Security Professional Exam
Certification Provider:	HP
Free Question Number:	62
Version:	v2025-07-15
# of views:	108
# of Questions views:	620
https://www.freepdfdumps.com/HP.HPE7-A02.v2025-07-15.q62.html	

NEW QUESTION: 1

Refer to the exhibit.



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

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

A. Disable OSPF entirely on VLANs 10-19.

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

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

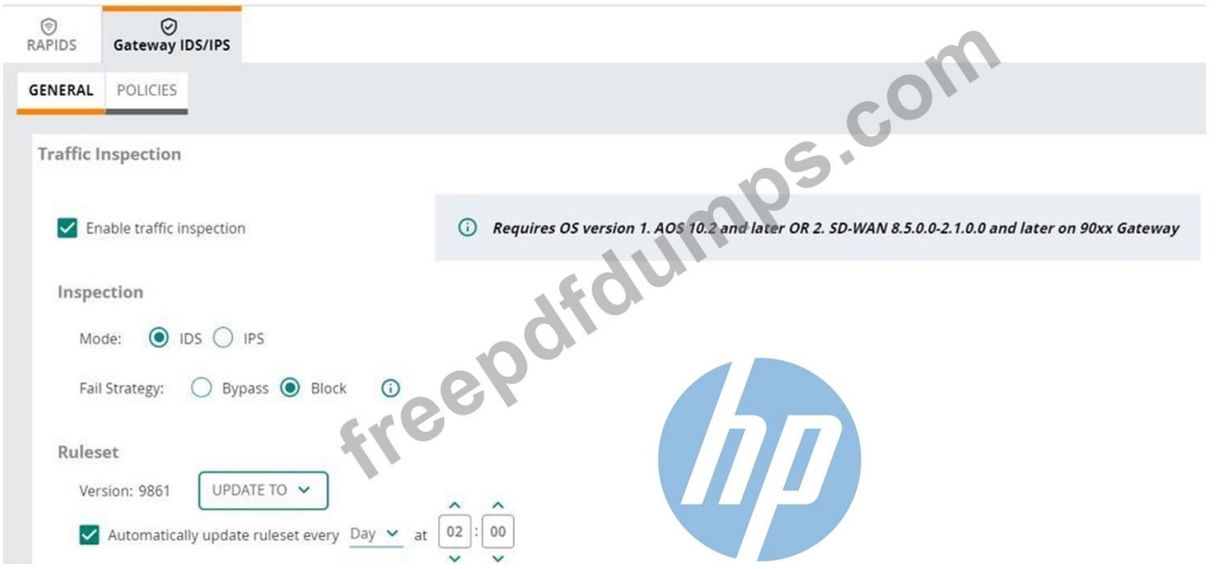
D. Configure passive-interface as the OSPF default and disable OSPF passive on Lag 1.

Answer: C (LEAVE A REPLY)

To prevent rogue OSPF routers in the network shown in the exhibit, the preferred configuration on Switch-2 is to configure OSPF authentication on Lag 1 in MD5 mode. This setup enhances security by ensuring that only routers with the correct MD5 authentication credentials can participate in the OSPF routing process. This method protects the OSPF sessions against unauthorized devices that might attempt to introduce rogue routing information into the network.
1.OSPF Authentication: Implementing MD5 authentication on Lag 1 ensures that OSPF updates are secured with a cryptographic hash. This prevents unauthorized OSPF routers from establishing peering sessions and injecting potentially malicious routing information.
2.Secure Communication: MD5 authentication provides a higher level of security compared to simple password authentication, as it uses a more robust hashing algorithm.
3.Applicability: Lag 1 is the primary link between Switch-1 and Switch-2, and securing this link helps protect the integrity of the OSPF routing domain.

NEW QUESTION: 2

Refer to the exhibit.



(Note that the HPE Aruba Networking Central interface shown here might look slightly different from what you see in your HPE Aruba Networking Central interface as versions change; however, similar concepts continue to apply.) An HPE Aruba Networking 9x00 gateway is part of an HPE Aruba Networking Central group that has the settings shown in the exhibit. What would cause the gateway to drop traffic as part of its IDPS settings?

A. Its site-to-site VPN connections failing

B. Traffic matching a rule in the active ruleset

C. Its IDPS engine failing

D. Traffic showing anomalous behavior

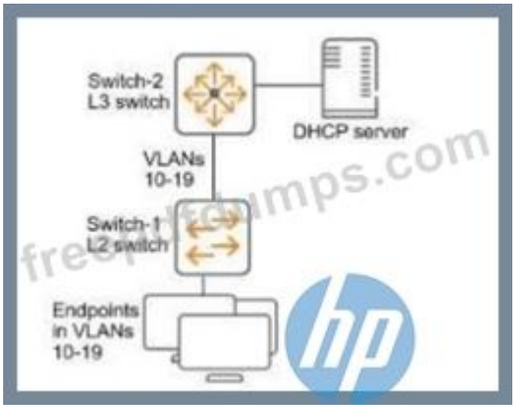
Answer: (SHOW ANSWER)

In the exhibit, the HPE Aruba Networking Central settings for the 9x00 gateway show that traffic inspection is enabled, and the gateway is set to operate in IDS (Intrusion Detection System)

mode with the fail strategy set to "Block". This configuration means that the gateway will drop traffic if it matches a rule in the active ruleset.
1.Active Ruleset: The ruleset version 9861 is active, and the gateway is configured to automatically update the ruleset daily.
2.Traffic Matching Rules: When traffic matches a rule in the active ruleset, it is flagged as suspicious or malicious.
3.Block Mode: Since the fail strategy is set to "Block", any traffic that matches a rule in the active ruleset will be dropped to prevent potential threats.

NEW QUESTION: 3
What correctly describes an HPE Aruba Networking AP's Device (TPM) certificate?
A. It is signed by an HPE Aruba Networking CA and is trusted by many HPE Aruba Networking solutions.
B. It works well as a captive portal certificate for guest SSIDs.
C. It is a self-signed certificate that should not be used in production.
D. It is installed on APs after they connect to and are provisioned by HPE Aruba Networking Central.
Answer: (SHOW ANSWER)
An HPE Aruba Networking AP's Device (TPM) certificate is signed by an HPE Aruba Networking Certificate Authority (CA) and is trusted by many HPE Aruba Networking solutions. This certificate is used for secure communications and device authentication within the Aruba network ecosystem.
1.CA-Signed Certificate: The Device (TPM) certificate is signed by a trusted Aruba CA, ensuring its authenticity and integrity.
2.Trust Across Solutions: Because it is signed by an Aruba CA, it is recognized and trusted by various Aruba solutions, facilitating secure interactions and communications.
3.Security: Using a CA-signed certificate enhances the security of the network by preventing unauthorized access and ensuring that communications are secure.

NEW QUESTION: 4
Refer to the exhibit.



You have verified that AOS-CX Switch-1 has constructed an IP-to-MAC binding table in VLANs 10-19.
Now you need to enable ARP inspection for the endpoint connected to Switch-1. What must you do first to prevent traffic disruption?
A. Configure ARP inspection on VLANs 10-19 on Switch-2.
B. Configure DHCP snooping on VLANs 10-19 on Switch-2.
C. Configure Switch-1 uplinks as trusted ARP inspection ports.
D. Create a static IP-to-MAC binding on Switch-1 for the DHCP server.
Answer: C (LEAVE A REPLY)
Dynamic ARP Inspection (DAI):
* ARP inspection verifies ARP packets against a trusted IP-to-MAC binding table to prevent ARP spoofing attacks.
* DHCP snooping is required to construct the IP-to-MAC binding table dynamically.
* To avoid traffic disruption, uplink ports that connect to trusted switches, DHCP servers, or routers must be explicitly configured as trusted ports for ARP inspection.
Steps to Prevent Traffic Disruption:
* Trust the Uplinks: ARP inspection must treat uplink ports as trusted to allow ARP traffic from legitimate DHCP servers and upstream switches.
* Enable DHCP Snooping: DHCP snooping must be enabled on Switch-2 to ensure consistent IP-to- MAC bindings upstream.
Why the Answer is Correct:
* Option A: Incorrect. ARP inspection on Switch-2 is important but not required first to prevent disruption on Switch-1.
* Option B: Incorrect. DHCP snooping must be enabled upstream eventually, but this alone will not stop immediate traffic disruption on Switch-1.
* Option C: Correct. Switch-1 uplinks must be trusted ARP inspection ports first to allow legitimate upstream traffic and prevent ARP disruption.
* Option D: Incorrect. Static bindings are not required if DHCP snooping is enabled, and they are manual, limiting scalability.
Conclusion:
To avoid traffic disruption, configure Switch-1 uplinks as trusted ARP inspection ports to ensure valid ARP traffic can pass upstream and downstream.

NEW QUESTION: 5
HPE Aruba Networking Central displays an alert about an Infrastructure Attack that was detected. You go to the Security > RAPIDS events and see that the attack was "Detect adhoc using Valid SSID." What is one possible next step?
A. Use HPE Aruba Networking Central floorplans or the detecting AP identities to locate the general area for the threat.
B. Look for the IP address associated with the offender and then check for that IP address among HPE Aruba Networking Central clients.

C. Make sure that you have tuned the threshold for that check, as false positives are common for it.
D. Make sure that clients have updated drivers, as faulty drivers are a common explanation for this attack type.
Answer: (SHOW ANSWER)
When HPE Aruba Networking Central detects an Infrastructure Attack, such as "Detect adhoc using Valid SSID," the next step is to locate the general area of the threat. You can use HPE Aruba Networking Central floorplans or the identities of the detecting APs to pinpoint the approximate location of the adhoc network.
This allows you to physically investigate and address the source of the threat, ensuring that unauthorized or rogue networks are quickly identified and mitigated.

NEW QUESTION: 6
A company uses HPE Aruba Networking ClearPass Policy Manager (CPPM) and HPE Aruba Networking ClearPass Device Insight (CPDI) and has integrated the two. CPDI admins have created a tag. CPPM admins have created rules that use that tag in the wired 802.1X and wireless 802.1X services' enforcement policies.
The company requires CPPM to apply the tag-based rules to a client directly after it learns that the client has that tag.
What is one of the settings that you should verify on CPPM?
A. The "Device Sync" setting is set to 1 in the ClearPass Device Insight Integration settings.
B. Both 802.1X services have the "Profile Endpoints" option enabled and an appropriate CoA profile selected in the Profiler tab.
C. Both 802.1X services have the "Use cached Role and Posture attributes from the previous sessions" setting.
D. The "Polling Interval" is set to 1 in the ClearPass Device Insight Integration settings.
Answer: B (LEAVE A REPLY)
To ensure that HPE Aruba Networking ClearPass Policy Manager (CPPM) applies tag-based rules to a client immediately after learning the client has that tag, verify that both 802.1X services have the "Profile Endpoints" option enabled and an appropriate Change of Authorization (CoA) profile selected in the Profiler tab. This setup ensures that when a device is profiled and tagged, CPPM can immediately enforce the updated policies through CoA.
1.Profile Endpoints: Enabling this option ensures that endpoint profiling is active, allowing CPPM to gather and use device information dynamically.
2.CoA Profile: Selecting an appropriate CoA profile ensures that CPPM can push policy changes immediately to the network devices, applying the new rules without delay.
3.Real-Time Enforcement: This configuration allows for the immediate application of new tags and associated policies, ensuring compliance with security requirements.

NEW QUESTION: 7

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

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

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

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

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

Answer: B (LEAVE A REPLY)

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

Explanation of Each Option

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

* Incorrect:
* Quarantining clients based on detected threats is typically managed by endpoint detection and response (EDR) solutions or next-generation firewalls (NGFWs).
* While an SWG can monitor and block risky web activity, it does not manage threat quarantine actions directly.

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

* Correct:
* SWGs monitor and control web traffic to block malicious websites and prevent exposure to malware.
* They enforce web usage policies even when users work remotely, protecting against phishing, drive-by downloads, and other web-based threats.
* With the proliferation of hybrid work environments, an SWG ensures that users are protected from risky sites regardless of their location.

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

* Incorrect:
* This use case falls under secure access service edge (SASE) solutions with Zero Trust Network Access (ZTNA), not an SWG.
* ZTNA focuses on granting secure, conditional access to applications, while SWGs focus on internet traffic security.

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

* Incorrect:
* Data loss prevention (DLP) tools or cloud access security brokers (CASBs) are designed for monitoring and preventing data exfiltration from SaaS applications.
* While SWGs can block access to specific websites or categories, they do not offer advanced DLP capabilities for SaaS environments.
References
* Aruba Secure Web Gateway Documentation.
* HPE Aruba SASE Solutions Guide.
* Best Practices for Hybrid Workforce Security with Aruba SWG.

NEW QUESTION: 8
A company assigns a different block of VLAN IDs to each of its access layer AOS-CX switches. The switches run version 10.07. The IDs are used for standard purposes, such as for employees, VoIP phones, and cameras. The company wants to apply 802.1X authentication to HPE Aruba Networking ClearPass Policy Manager (CPPM) and then steer clients to the correct VLANs for local forwarding.
What can you do to simplify setting up this solution?
A. Assign consistent names to VLANs of the same type across the AOS-CX switches and have user-roles reference names.
B. Use the trunk allowed VLAN setting to assign multiple VLAN IDs to the same role.
C. Change the VLAN IDs across the AOS-CX switches so that they are consistent.
D. Avoid configuring the VLAN in the role; use trunk VLANs to assign multiple VLANs to the port instead.
Answer: A (LEAVE A REPLY)
To simplify the setup of 802.1X authentication with HPE Aruba Networking ClearPass Policy Manager (CPPM) and ensure clients are steered to the correct VLANs for local forwarding, you should assign consistent names to VLANs of the same type across the AOS-CX switches and have user-roles reference these names. This approach allows for a more straightforward configuration and management process, as the user roles can apply consistent policies based on VLAN names rather than specific IDs. It also helps in maintaining clarity and reducing errors in VLAN assignments across different switches.

NEW QUESTION: 9
What is a typical use case for using HPE Aruba Networking ClearPass Onboard to provision devices?
A. Enabling unmanaged devices to succeed at certificate-based 802.1X
B. Enabling managed Windows domain computers to succeed at certificate-based 802.1X
C. Enhancing security for IoT devices that need to authenticate with MAC-Auth
D. Enforcing posture-based assessment on managed Windows domain computers
Answer: A (LEAVE A REPLY)

A typical use case for using HPE Aruba Networking ClearPass Onboard is to provision unmanaged devices to succeed at certificate-based 802.1X authentication. ClearPass Onboard allows users to securely configure their personal devices with the necessary certificates and network settings to authenticate on the network using 802.1X, which enhances security and simplifies the onboarding process for unmanaged devices.
1.Certificate-Based Authentication: ClearPass Onboard simplifies the process of issuing and installing certificates on unmanaged devices, ensuring they can authenticate securely using 802.1X.
2.User-Friendly Onboarding: The Onboard process is user-friendly, guiding users through the steps needed to configure their devices for network access.
3.Enhanced Security: By using certificates for authentication, the solution provides a higher level of security compared to traditional username/password methods.

NEW QUESTION: 10
Which statement describes Zero Trust Security?
A. Companies must apply the same access controls to all users, regardless of identity.
B. Companies that support remote workers cannot achieve zero trust security and must determine if the benefits outweigh the cost.
C. Companies should focus on protecting their resources rather than on protecting the boundaries of their internal network.
D. Companies can achieve zero trust security by strengthening their perimeter security to detect a wider range of threats.
Answer: C (LEAVE A REPLY)
What is Zero Trust Security?
* Zero Trust Security is a security model that operates on the principle of "never trust, always verify."
* It focuses on securing resources (data, applications, systems) and continuously verifying the identity and trust level of users and devices, regardless of whether they are inside or outside the network.
* The primary aim is to reduce reliance on perimeter defenses and implement granular access controls to protect individual resources.
Analysis of Each Option
A: Companies must apply the same access controls to all users, regardless of identity:
* Incorrect:
* Zero Trust enforces dynamic and identity-based access controls, not the same static controls for everyone.
* Users and devices are granted access based on their specific context, role, and trust level.
B: Companies that support remote workers cannot achieve zero trust security and must determine if the benefits outweigh the cost:
* Incorrect:

* Zero Trust is particularly effective for securing remote work environments by verifying and authenticating remote users and devices before granting access to resources.
* The model is adaptable to hybrid and remote work scenarios, making this statement false.
C: Companies should focus on protecting their resources rather than on protecting the boundaries of their internal network:
* Correct:
* Zero Trust shifts the focus from perimeter security (traditional network boundaries) to protecting specific resources.
* This includes implementing measures such as:
* Micro-segmentation.
* Continuous monitoring of user and device trust levels.
* Dynamic access control policies.
* The emphasis is on securing sensitive assets rather than assuming an internal network is inherently safe.
D: Companies can achieve zero trust security by strengthening their perimeter security to detect a wider range of threats:
* Incorrect:
* Zero Trust challenges the traditional reliance on perimeter defenses (firewalls, VPNs) as the sole security mechanism.
* Strengthening perimeter security is not sufficient for Zero Trust, as this model assumes threats can already exist inside the network.
Final Explanation
Zero Trust Security emphasizes protecting resources at the granular level rather than relying on the traditional security perimeter, which makes C the most accurate description.
References
* NIST Zero Trust Architecture Guide.
* Zero Trust Principles and Implementation in Modern Networks by HPE Aruba.
* "Never Trust, Always Verify" Framework Overview from Cybersecurity Best Practices.

NEW QUESTION: 11
What is one use case for implementing user-based tunneling (UBT) on AOS-CX switches?
A. Centralizing the distribution of wired traffic without requiring HPE Aruba Networking gateways
B. Tunneling traffic directly to a third-party firewall in a client data center
C. Adding 802.1X while continuing to use the existing VLAN and ACL structure in the Ethernet network
D. Applying enhanced security features such as deep packet inspection (DPI) to wired traffic
Answer: D (LEAVE A REPLY)
Implementing user-based tunneling (UBT) on AOS-CX switches is beneficial for applying enhanced security features such as deep packet inspection (DPI) to wired traffic. UBT allows the traffic from specific users or devices to be tunneled to a central controller or security appliance where advanced security policies, including DPI, can be applied. This approach ensures that

even wired traffic benefits from the same level of security and inspection typically available for wireless traffic, thus enhancing overall network security.

NEW QUESTION: 12
A company issues user certificates to domain computers using its Windows CA and the default user certificate template. You have set up HPE Aruba Networking ClearPass Policy Manager (CPPM) to authenticate 802.1X clients with those certificates. However, during tests, you receive an error that authorization has failed because the usernames do not exist in the authentication source.
What is one way to fix this issue and enable clients to successfully authenticate with certificates?
A. Configure rules to strip the domain name from the username.
B. Change the authentication method list to include both PEAP MSCHAPv2 and EAP-TLS.
C. Add the ClearPass Onboard local repository to the authentication source list.
D. Remove EAP-TLS from the authentication method list and add TEAP there instead.
Answer: A (LEAVE A REPLY)
To fix the issue where authorization fails because the usernames do not exist in the authentication source, you can configure rules in HPE Aruba Networking ClearPass Policy Manager (CPPM) to strip the domain name from the username. When certificates are issued by a Windows CA, the username in the certificate often includes the domain (e.g., user@domain.com). ClearPass might not be able to find this format in the authentication source. By stripping the domain name, you ensure that ClearPass searches for just the username (e.g., user) in the authentication source, allowing successful authentication.

NEW QUESTION: 13
A company uses HPE Aruba Networking ClearPass Device Insight (CPDI) (the standalone application option). In the details for a generic device cluster, you see a recommendation for "Windows 8/10" with 70% accuracy.
What does this mean?
A. CPDI has detected that these devices match about 70% of the system rule for defining "Windows 8/10" devices.
B. CPDI has matched these devices against several, conflicting system rules. 70% of those rules are for
"Windows 8/10" devices.
C. CPDI has grouped this cluster with similar classified devices. 70% of those classified devices are
"Windows 8/10."
D. CPDI has used MAC OUI to group these devices together. The average device's MAC address matches
70% of the "Windows 8/10" OUI.
Answer: (SHOW ANSWER)

When HPE Aruba Networking ClearPass Device Insight (CPDI) shows a recommendation for "Windows 8
/10" with 70% accuracy for a generic device cluster, it means that CPDI has detected that these devices match about 70% of the system rule criteria for defining "Windows 8/10" devices. This percentage indicates the confidence level based on the observed characteristics and behavior of the devices, helping administrators understand the likelihood that these devices are indeed running Windows 8 or 10.

NEW QUESTION: 14
A company has HPE Aruba Networking APs running AOS-10 and managed by HPE Aruba Networking Central. The company also has AOS-CX switches. The security team wants you to capture traffic from a particular wireless client. You should capture this client's traffic over a 15 minute time period and then send the traffic to them in a PCAP file.
What should you do?
A. Go to the client's AP in HPE Aruba Networking Central. Use the "Security" page to run a packet capture.
B. Access the CLI for the client's AP. Set up a mirroring session between its radio and a management station running Wireshark.
C. Access the CLI for the client's AP's switch. Set up a mirroring session between the AP's port and a management station running Wireshark.
D. Go to that client in HPE Aruba Networking Central. Use the "Live Events" page to run a packet capture.
Answer: A (LEAVE A REPLY)
To capture traffic from a particular wireless client for a 15-minute period and then send the traffic in a PCAP file, you should go to the client's AP in HPE Aruba Networking Central and use the "Security" page to run a packet capture. This method allows you to directly capture the client's traffic from the AP managing the wireless connection, ensuring that you gather the relevant traffic data for analysis.
1.Centralized Management: HPE Aruba Networking Central provides a centralized interface for managing and monitoring APs, making it easy to initiate packet captures.
2.Security Page: The "Security" page in Aruba Central includes tools for running packet captures, allowing you to specify the duration and other parameters.
3.Ease of Use: This approach simplifies the process by using the built-in features of Aruba Central, avoiding the need for complex CLI commands or additional hardware.

NEW QUESTION: 15
A company is using HPE Aruba Networking Central SD-WAN Orchestrator to establish a hub-spoke VPN between branch gateways (BGWs) at 1444 site and VPNCs at multiple data centers.
What is part of the configuration that admins need to complete?
A. At the global level, create default IPsec policies for the SD-WAN Orchestrator to use.
B. In BGWs' groups, select the VPNCs to which to connect in a DC preference list.

C. In VPNCs' groups, establish VPN pools to control which branches connect to which VPNCs.
D. In BGWs' and VPNCs' groups, create default IKE policies for the SD-WAN Orchestrator to use.
Answer: B (LEAVE A REPLY)
When using HPE Aruba Networking Central SD-WAN Orchestrator to establish a hub-spoke VPN between branch gateways (BGWs) and VPN concentrators (VPNCs) at multiple data centers, admins need to configure the BGWs' groups by selecting the VPNCs to which they should connect in a Data Center (DC) preference list. This configuration ensures that branch gateways are properly directed to the preferred VPN concentrators, optimizing the hub-spoke VPN topology.
1.DC Preference List: This list allows administrators to prioritize which data center VPNCs the BGWs should connect to, ensuring efficient routing and redundancy.
2.Hub-Spoke Configuration: Properly setting the DC preference list is essential for establishing the desired hub-spoke VPN architecture.
3.Optimized Connectivity: This setup helps in optimizing traffic flow and maintaining connectivity between branches and data centers.

NEW QUESTION: 16
You are configuring the HPE Aruba Networking ClearPass Device Insight Integration settings on ClearPass Policy Manager (CPPM). For which use case should you set the 'Tag Updates Action" to " apply for all tag updates"?
A. When the Device Insight integration poll interval is set to a relatively long interval but you still want CPPM to be informed quickly about devices' new tags.
B. When Device Insight tags are only used to identify dangerous devices, and you want to disconnect those devices without having to set up new rules in enforcement policies.
C. When CPPM is gathering posture information for CPDI, and you want CPDI to always have access to the most up-to-date information.
D. When you plan to have CPPM issue CoAs for clients with new tags, but do not want to have to list those specific tags in the Device Integration settings in advance.
Answer: (SHOW ANSWER)
* Tag Updates Action - "Apply for All Tag Updates":
* This setting ensures that all updated tags from Device Insight (CPDI) are applied dynamically.
* It is particularly useful when you want to trigger Change of Authorization (CoA) without explicitly predefining the tag values.
* Option D: Correct. This setting allows CPPM to issue CoAs automatically for updated tags without requiring prior configuration of specific tags.
* Option A: Incorrect. The setting is not directly related to reducing the poll interval latency.
* Option B: Incorrect. Disconnecting devices based on dangerous tags would require predefined enforcement rules.
* Option C: Incorrect. Posture information updates do not directly rely on this setting.

NEW QUESTION: 17
You have installed an HPE Aruba Networking Network Analytic Engine (NAE) script on an AOS-CX switch to monitor a particular function.
Which additional step must you complete to start the monitoring?
A. Reboot the switch.
B. Enable NAE, which is disabled by default.
C. Edit the script to define monitor parameters.
D. Create an agent from the script.
Answer: D (LEAVE A REPLY)
After installing an HPE Aruba Networking Network Analytic Engine (NAE) script on an AOS-CX switch, the additional step required to start the monitoring is to create an agent from the script. The agent is responsible for executing the script and collecting the monitoring data as defined by the script parameters.
1.Script Installation: Installing the script provides the logic and parameters for monitoring.
2.Agent Creation: Creating an agent from the script activates the monitoring process, allowing the NAE to begin tracking the specified function.
3.Operational Step: This step ensures that the monitoring logic is applied and the data collection starts as per the script's configuration.

NEW QUESTION: 18
You need to set up HPE Aruba Networking ClearPass Policy Manager (CPPM) to provide certificate-based authentication of 802.1X supplicants.
How should you upload the root CA certificate for the supplicants' certificates?
A. As a ClearPass Server certificate with the RADIUS/EAP usage
B. As a Trusted CA with the AD/LDAP usage
C. As a Trusted CA with the EAP usage
D. As a ClearPass Server certificate with the Database usage
Answer: C (LEAVE A REPLY)
To set up HPE Aruba Networking ClearPass Policy Manager (CPPM) for certificate-based authentication of
802.1X supplicants, you need to upload the root CA certificate as a Trusted CA with the EAP usage. This configuration allows the ClearPass server to validate the certificates presented by the supplicants during the

802.1X authentication process. By marking the certificate for EAP usage, ClearPass can properly authenticate the supplicant devices using the trusted certificate authority (CA) that issued their certificates.

NEW QUESTION: 19
An admin has configured an AOS-CX switch with these settings:
port-access role employees
vlan access name employees
This switch is also configured with CPPM as its RADIUS server.
Which enforcement profile should you configure on CPPM to work with this configuration?
A. RADIUS Enforcement type with HPE-User-Role VSA set to "employees"
B. HPE Aruba Networking Downloadable Role Enforcement type with role name set to "employees"
C. HPE Aruba Networking Downloadable Role Enforcement type with gateway role name set to "employees"
D. RADIUS Enforcement type with Aruba-User-Role VSA set to "employees"
Answer: D (LEAVE A REPLY)
To ensure that the AOS-CX switch properly assigns the "employees" role when using CPPM (ClearPass Policy Manager) as the RADIUS server, you should configure a RADIUS Enforcement profile on CPPM with the Aruba-User-Role VSA (Vendor-Specific Attribute) set to "employees". This configuration ensures that when an endpoint authenticates, CPPM sends the appropriate role assignment to the AOS-CX switch, which then applies the corresponding policies and VLAN settings defined for the "employees" role.

NEW QUESTION: 20
You have run an Active Endpoint Security Report on HPE Aruba Networking ClearPass. The report indicates that hundreds of endpoints have MAC addresses but no known IP addresses.
What is one step for addressing this issue?
A. Set up network devices to implement RADIUS accounting to CPPM.
B. Add CPPM's IP address to the IP helper list on routing switches.
C. Set up switches to implement ARP inspection on client VLANs.
D. Configure CPPM as a Syslog destination on network devices.
Answer: B (LEAVE A REPLY)
When the Active Endpoint Security Report on HPE Aruba Networking ClearPass indicates that endpoints have MAC addresses but no known IP addresses, one effective step to address this issue is to add CPPM's (ClearPass Policy Manager) IP address to the IP helper list on routing switches. This configuration ensures that DHCP requests are forwarded to the ClearPass server, allowing it to track and report the IP addresses assigned to the endpoints. This helps ClearPass maintain an accurate mapping of MAC addresses to IP addresses, improving endpoint visibility and security management.

NEW QUESTION: 21
An AOS-CX switch has been configured to implement UBT to two HPE Aruba Networking gateways that implement VRRP on the users' VLAN. What correctly describes how the switch tunnels UBT users' traffic to those gateways?
A. The switch always sends the users' traffic to the VRRP master.
B. The switch always sends all users' traffic to the primary gateway configured in the UBT zone.
C. The switch always load shares the users' traffic across both gateways.
D. The switch always sends all users' traffic to the gateway assigned as the active device designed gateway.
Answer: B (LEAVE A REPLY)
* User-Based Tunneling (UBT) with VRRP:
* UBT allows traffic from authenticated users to be tunneled to an HPE Aruba Networking gateway.
* In the case of VRRP, where two gateways are configured for redundancy, the AOS-CX switch will always send the traffic to the primary gateway defined in the UBT zone configuration.
* The VRRP state (master/backup) does not impact the UBT decision; the UBT primary configuration takes precedence.
* Option Analysis:
* Option A: Incorrect. UBT does not strictly follow the VRRP master; it adheres to the UBT primary gateway configuration.
* Option B: Correct. The switch tunnels all traffic to the primary gateway configured in the UBT zone.
* Option C: Incorrect. UBT does not load-share traffic between gateways.
* Option D: Incorrect. UBT uses the primary gateway configured in the UBT zone, not dynamically determined active devices.

NEW QUESTION: 22
A port-access role for AOS-CX switches has this policy applied to it:
plaintext
Copy code
port-access policy mypolicy
10 class ip zoneC action drop
20 class ip zoneA action drop
100 class ip zoneB
The classes have this configuration:
plaintext
Copy code
class ip zoneC
10 match tcp 10.2.0.0/16 eq https
class ip zoneA
10 match ip any 10.1.0.0/16

class ip zoneB
10 match ip any 10.0.0.0/8
The company wants to permit clients in this role to access 10.2.12.0/24 with HTTPS. What should you do?
A. Add this rule to zoneC: 5 match any 10.2.12.0/24 eq https
B. Add this rule to zoneA: 5 ignore tcp any 10.2.12.0/24 eq https
C. Add this rule to zoneB: 5 match tcp any 10.2.12.0/24 eq https
D. Add this rule to zoneC: 5 ignore tcp any 10.2.12.0/24 eq https
Answer: A (LEAVE A REPLY)
Comprehensive Detailed Explanation
* The requirement is to permit HTTPS traffic from clients to the 10.2.12.0/24 subnet.
* ZoneC is configured to drop all HTTPS traffic to the 10.2.0.0/16 subnet. Therefore, the first match in the zoneC class (priority 10) will drop the desired traffic.
* To override this behavior, you must add a higher-priority rule (lower rule number) to zoneC that explicitly matches 10.2.12.0/24 and permits the traffic.
Thus, adding the rule 5 match any 10.2.12.0/24 eq https to zoneC ensures the desired traffic is permitted while maintaining the drop behavior for the rest of 10.2.0.0/16.
References
* AOS-CX Role-Based Access Control documentation.
* Understanding class priority and policy rule ordering in AOS-CX.

NEW QUESTION: 23
A company has several use cases for using its AOS-CX switches' HPE Aruba Networking Network Analytics Engine (NAE).
What is one guideline to keep in mind as you plan?
A. Each switch model has a maximum number of supported monitors, and one agent might have multiple monitors.
B. You can install multiple scripts on a switch, but you can deploy only one agent per script.
C. The switch will permit you to deploy as many NAE agents as you want, but they might degrade the switch functionality.
D. When you use custom scripts, you can create as many agents from each script as you want.
Answer: A (LEAVE A REPLY)
The Network Analytics Engine (NAE) in AOS-CX switches provides intelligent monitoring, troubleshooting, and performance analysis through predefined or custom scripts. Here's an analysis of the guidelines for NAE:
A: Each switch model has a maximum number of supported monitors, and one agent might have multiple monitors.
* Correct:
* Each AOS-CX switch model has hardware and software limitations, including the number of agents and monitors it supports.

* Monitors are data collection points for tracking specific metrics like interface statistics, CPU usage, or custom-defined parameters.
* Agents are scripts that use monitors to evaluate data, trigger actions, or generate alerts.
* Since one agent can have multiple monitors, the total number of monitors might impact the scalability of agents.
B: You can install multiple scripts on a switch, but you can deploy only one agent per script.
* Incorrect:
* Multiple agents can be deployed from the same script if they monitor different parameters or have different configurations.
* The limitation is usually related to the total number of agents and monitors supported by the switch model, not the script itself.
C: The switch will permit you to deploy as many NAE agents as you want, but they might degrade the switch functionality.
* Incorrect:
* AOS-CX enforces hardware and software limits on the number of agents and monitors. These limits are designed to prevent degradation of switch performance.
* You cannot deploy an unlimited number of agents, as the system enforces these restrictions.
D: When you use custom scripts, you can create as many agents from each script as you want.
* Incorrect:
* While you can use custom scripts to create agents, the total number of agents is subject to the switch's maximum supported limits.
* The scalability of agents is still bound by hardware and software constraints, even with custom scripts.
References
* HPE Aruba AOS-CX Network Analytics Engine Configuration Guide.
* Aruba AOS-CX Switch Series Technical Specifications.
* Best Practices for NAE Deployment in AOS-CX Networks.

NEW QUESTION: 24
HPE Aruba Networking Central displays a Gateway Threat Count alert in the alert list. How can you gather more information about what caused the alert to trigger?
A. Use HPE Aruba Networking Central tools to run a Network Check on the gateway with which the alert is associated.
B. Use Live Monitoring on the gateway to download a packet capture of recent traffic flowing through the gateway.
C. Check the threat list for the gateway associated with the alert. Access threat details and download packet info.
D. Check the gateway's Audit Trail in HPE Aruba Networking Central for more details about the threats that triggered the alert.
Answer: C (LEAVE A REPLY)
Gateway Threat Count Alert

This alert indicates that the gateway has detected threats in traffic passing through it. HPE Aruba Networking Central provides tools to investigate and analyze these threats in detail.
Analysis of Each Option
A: Use HPE Aruba Networking Central tools to run a Network Check on the gateway with which the alert is associated:
* Incorrect:
* Network Check tools in Central are primarily used for connectivity and performance diagnostics, not for analyzing detected threats.
* This does not provide insight into the specific threats triggering the Gateway Threat Count alert.
B: Use Live Monitoring on the gateway to download a packet capture of recent traffic flowing through the gateway:
* Incorrect:
* Live Monitoring and packet capture can provide raw traffic data, but interpreting this requires significant manual analysis.
* The Gateway Threat Count alert already provides summarized threat insights that are easier to access via the threat list.
C: Check the threat list for the gateway associated with the alert. Access threat details and download packet info:
* Correct:
* The threat list is specifically designed to display detailed information about detected threats, such as their type, severity, and source/destination.
* Administrators can access this list in Central for the affected gateway, view granular details, and even download associated packet data for deeper inspection.
D: Check the gateway's Audit Trail in HPE Aruba Networking Central for more details about the threats that triggered the alert:
* Incorrect:
* The Audit Trail tracks configuration changes and administrative actions, not the details of detected threats.
* It is not relevant for investigating the Gateway Threat Count alert.
Final Recommendation
To gather more information about what caused the Gateway Threat Count alert to trigger, check the threat list for the associated gateway. This provides detailed threat information and the option to download packet data for further analysis.
References
* HPE Aruba Networking Central Threat Management Guide.
* Understanding Gateway IDS/IPS Alerts in Aruba Central Documentation.
* Best Practices for Threat Investigation Using Aruba Central.

NEW QUESTION: 25

A company has AOS-CX switches and HPE Aruba Networking ClearPass Policy Manager (CPPM). The company wants switches to implement 802.1X authentication to CPPM and download user roles.
What is one task that you must complete on the switches to support this use case?
A. Specify CPPM as the RADIUS server with the exact CN in CPPM's HTTPS certificate.
B. Install the root CA certificate for CPPM's RADIUS certificate in a TA profile on the switches.
C. Configure empty user-roles with names that match enforcement profile names on CPPM.
D. Specify a ClearPass username and password that match the name and RADIUS secret in a CPPM network device entry.
Answer: B (LEAVE A REPLY)
To support 802.1X authentication and download user roles from HPE Aruba Networking ClearPass Policy Manager (CPPM) on AOS-CX switches, you must install the root CA certificate for CPPM's RADIUS certificate in a Trust Anchor (TA) profile on the switches. This ensures that the switches trust the RADIUS server certificate presented by CPPM during the authentication process.
1.Root CA Certificate: Installing the root CA certificate ensures that the switch can verify the authenticity of the RADIUS server certificate provided by CPPM.
2.Trust Anchor Profile: The TA profile on the switch holds the root CA certificate, establishing a trust relationship between the switch and the CPPM RADIUS server.
3.Secure Authentication: This setup is essential for securing the 802.1X authentication process and enabling the download of user roles.

NEW QUESTION: 26
What is one use case that companies can fulfill using HPE Aruba Networking ClearPass Policy Manager's (CPPM's) Device Profiler?
A. OIdentifying device security vulnerabilities by CVE ID and receiving remediation recommendations
B. Leveraging artificial intelligence to more accurately identify Internet of Things (IoT) devices
C. Quarantining devices that do not have the required antivirus software installed on them
D. Assigning different AOS firewall roles to users on computers and the same users on smartphones
Answer: B (LEAVE A REPLY)
One use case that companies can fulfill using HPE Aruba Networking ClearPass Policy Manager's (CPPM's) Device Profiler is leveraging artificial intelligence to more accurately identify Internet of Things (IoT) devices. ClearPass Device Profiler uses AI and machine learning to analyze network traffic and device behavior, providing detailed and accurate identification of IoT devices on the network. This helps in managing and securing diverse and numerous IoT devices by ensuring they are correctly profiled and assigned appropriate access policies.

NEW QUESTION: 27

A company has been running Gateway IDS/IPS on its gateways in IDS mode for several weeks. The company wants to transition to IPS mode.
What is one step you should recommend?
A. Disable traffic inspection and reboot before re-enabling traffic inspection with the new mode.
B. Change the mode on one gateway at a time to establish a smoother transition period.
C. Consider applying a stricter IPS policy to minimize issues during the transition period.
D. Check for legitimate traffic that has been flagged as a threat and allow list the associated rules.
Answer: D (LEAVE A REPLY)
When transitioning from Intrusion Detection System (IDS) mode to Intrusion Prevention System (IPS) mode, it's critical to review and refine configurations to ensure legitimate traffic is not blocked. Here's the reasoning behind each option:
A: Disable traffic inspection and reboot before re-enabling traffic inspection with the new mode.
* Incorrect:
* Transitioning to IPS mode does not require a full reboot or disabling traffic inspection.
* This step is unnecessary and could lead to downtime that impacts network operations.
B: Change the mode on one gateway at a time to establish a smoother transition period.
* Incorrect:
* While a phased approach might help in some large deployments, it does not directly address the potential for legitimate traffic to be blocked by IPS mode.
* IPS operates in real-time, so misconfigured rules or policies need to be addressed before enabling IPS on any gateway.
C: Consider applying a stricter IPS policy to minimize issues during the transition period.
* Incorrect:
* A stricter IPS policy increases the likelihood of false positives, which could disrupt legitimate business-critical traffic.
* During the transition, the focus should be on minimizing disruptions by fine-tuning policies, not making them stricter.
D: Check for legitimate traffic that has been flagged as a threat and allow list the associated rules.
* Correct:
* In IDS mode, the system only detects and logs suspicious traffic but does not block it.
Reviewing these logs for false positives allows the organization to fine-tune policies and allow list legitimate traffic before transitioning to IPS mode.
* By doing this, the company ensures that IPS mode will block actual threats while permitting legitimate traffic.
* This is a proactive step to prevent unnecessary disruptions to normal operations when IPS mode is enabled.
References
* HPE Aruba Gateway IDS/IPS Configuration Guide.
* Best Practices for Transitioning from IDS to IPS Modes in Aruba Networks.
* Aruba Network Threat Management Documentation.

NEW QUESTION: 28
A security team needs to track a device's communication patterns and identify patterns such as how many destinations the device is accessing.
Which Aruba solution can show this information at a glance?
A. HPE Aruba Networking ClearPass Insight Endpoints and Network Dashboards
B. HPE Aruba Networking ClearPass Policy Manager (CPPM) live monitoring Access Tracker
C. HPE Aruba Networking ClearPass Device Insight (CPDI) under a device's network activity
D. AOS-CX Analytics Dashboard using the system-installed NAE agent
Answer: (SHOW ANSWER)
HPE Aruba Networking ClearPass Device Insight (CPDI) can show detailed information about a device's communication patterns, including how many destinations the device is accessing. CPDI provides comprehensive visibility into the behavior and activity of devices on the network, allowing the security team to track and analyze communication patterns at a glance. This information is critical for identifying anomalies and potential security threats.

NEW QUESTION: 29
A company has AOS-CX switches. The company wants to make it simpler and faster for admins to detect denial of service (DoS) attacks, such as ping or ARP floods, launched against the switches.
What can you do to support this use case?
A. Deploy an NAE agent on the switches to monitor control plane policing (CoPP).
B. Implement ARP inspection on all VLANs that support end-user devices.
C. Configure the switches to implement RADIUS accounting to HPE Aruba Networking ClearPass and enable HPE Aruba Networking ClearPass Insight.
D. Enabling debugging of security functions on the switches.
Answer: (SHOW ANSWER)
To support the detection of denial of service (DoS) attacks on AOS-CX switches, deploying an NAE (Network Analytics Engine) agent to monitor control plane policing (CoPP) is the best approach. NAE agents provide real-time analytics and monitoring capabilities, allowing administrators to detect anomalies and potential DoS attacks, such as ping or ARP floods, more quickly and efficiently. Control plane policing helps protect the switch's CPU from unnecessary or malicious traffic, and the NAE agent can alert administrators when thresholds are exceeded, providing a proactive measure to detect and mitigate DoS attacks.

NEW QUESTION: 30
A company needs you to integrate HPE Aruba Networking ClearPass Policy Manager (CPPM) with HPE Aruba Networking ClearPass Device Insight (CPDI).
What is one task you should do to prepare?
A. Install the root CA for CPPM's HTTPS certificate as trusted in the CPDI application.
B. Configure WMI, SSH, and SNMP external accounts for device scanning on CPPM.
C. Enable Insight in the CPPM server configuration settings.

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

Answer: C (LEAVE A REPLY)

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

1.Insight Enablement: Enabling Insight on the CPPM server allows it to leverage the data and capabilities of CPDI, integrating device profiling information into policy decisions.

2.Data Sharing: This integration ensures that CPPM can receive and use detailed device information from CPDI to make more informed policy enforcement decisions.

3.Configuration: Properly configuring the server settings to enable Insight ensures seamless communication and data flow between CPPM and CPDI.

NEW QUESTION: 31

A company has AOS-CX switches, which authenticate clients to HPE Aruba Networking ClearPass Policy Manager (CPPM). CPPM is set up to receive a variety of information about clients' profile and posture. New information can mean that CPPM should change a client's enforcement profile. What should you set up on the switches to help the solution function correctly?

A. Enable RADIUS accounting to CPPM, including interim RADIUS accounting.

B. Configure a RADIUS track that references CPPM's FQDN or IP address.

C. Enable dynamic authorization, and specify CPPM as a dynamic authorization client.

D. Re-configure the authentication server on the switch specifying CPPM as a TACACS server.

Answer: C (LEAVE A REPLY)

* Dynamic Authorization for Enforcement Profile Updates:
* When CPPM receives updated client posture or profile data, it can initiate a Change of Authorization (CoA) to update enforcement profiles dynamically.
* To support this:
* Dynamic Authorization must be enabled on the switches.
* CPPM must be configured as a dynamic authorization client to send CoA requests.
* Option C: Correct. Dynamic authorization ensures that the switch can apply updated enforcement profiles based on new information from CPPM.
* Option A: Incorrect. RADIUS accounting provides session updates but does not enable dynamic changes to enforcement profiles.
* Option B: Incorrect. RADIUS track is for monitoring RADIUS server availability, not dynamic enforcement updates.
* Option D: Incorrect. TACACS is not used for dynamic authorization; RADIUS handles this functionality.

NEW QUESTION: 32
You are using Wireshark to view packets captured from HPE Aruba Networking infrastructure, but you're not sure that the packets are displaying correctly. In which circumstance does it make sense to configure Wireshark to ignore protection bits with the IV for the 802.11 protocol?
A. When the traffic was captured on the data plane of an HPE Aruba Networking gateway and sent to a remote IP.
B. When the traffic was mirrored from an AOS-CX switch port connected to an AP.
C. When the traffic was captured from an AP with HPE Aruba Networking Central.
D. When the traffic was captured on the control plane of an HPE Aruba Networking MC and sent to a remote IP.
Answer: C (LEAVE A REPLY)
* 802.11 Traffic and Protection Bits:
* In the 802.11 protocol, protection bits and the Initialization Vector (IV) are used in encrypted wireless traffic.
* If the traffic is captured directly from an AP, the frames may include encrypted content.
* Wireshark may misinterpret these protection bits or fail to display the frames correctly unless it is configured to ignore protection bits and correctly parse the IV.
* Key Scenario:
* When traffic is captured directly from an AP managed by HPE Aruba Networking Central, the frames are often captured before decryption occurs.
* In such cases, you must configure Wireshark to ignore the protection bits and handle the IV properly for correct frame interpretation.
* Option Analysis:
* Option A: Incorrect. Data plane traffic sent to a remote IP is usually decrypted, so Wireshark does not require this adjustment.
* Option B: Incorrect. Switch port mirroring captures traffic at Layer 2/3, not raw 802.11 frames.
* Option C: Correct. Traffic captured directly from an AP via HPE Aruba Networking Central often includes encrypted wireless frames, requiring Wireshark adjustments.
* Option D: Incorrect. Control plane traffic is typically management data and not raw wireless frames needing IV interpretation.

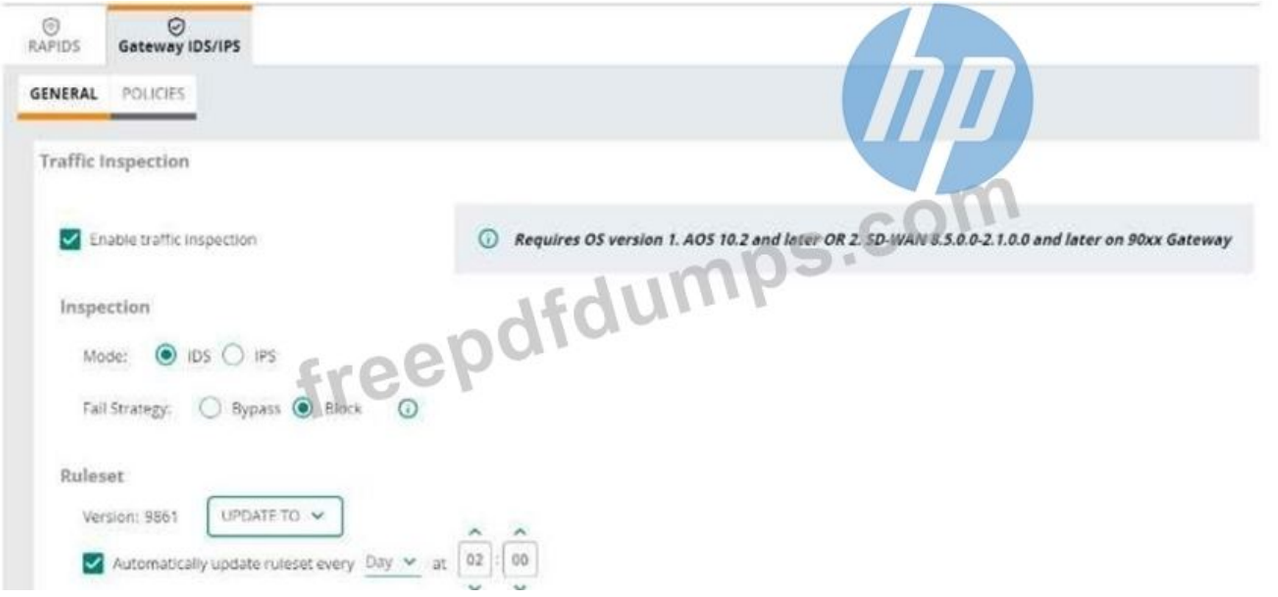
NEW QUESTION: 33

A company wants to turn on Wireless IDS/IPS infrastructure and client detection at the high level on HPE Aruba Networking APs. The company does not want to enable any prevention settings. What should you explain about HPE Aruba Networking recommendations?
A. HPE Aruba Networking recommends turning on both wired and wireless prevention whenever you enable detection at high.
B. HPE Aruba Networking recommends using hybrid AP mode, as opposed to Air Monitors (AMs), when implementing detection without prevention.
C. HPE Aruba Networking recommends disabling client detection when you configure infrastructure detection at high, as infrastructure detection includes all the client checks and more.
D. HPE Aruba Networking recommends configuring infrastructure and client detection at a custom level and disabling or tuning some of the settings that are likely to produce false positives.
Answer: D (LEAVE A REPLY)
When enabling Wireless IDS/IPS infrastructure and client detection at a high level on HPE Aruba Networking APs without enabling prevention settings, HPE Aruba Networking recommends configuring detection at a custom level and adjusting settings to minimize false positives. This approach allows for effective monitoring while reducing the risk of unnecessary alerts and maintaining the accuracy of detections.
1.Custom Level Configuration: By customizing the detection settings, you can tailor the system to your specific environment, ensuring that only relevant threats are detected and reducing false positives.
2.False Positive Reduction: Disabling or tuning settings that are likely to produce false positives helps in maintaining the reliability of the detection system and prevents alert fatigue.
3.Focused Detection: Custom configuration ensures that the IDS/IPS focuses on critical detections, improving overall security posture.

NEW QUESTION: 34
You are using OpenSSL to obtain a certificate signed by a Certification Authority (CA). You have entered this command:
openssl req -new -out file1.pem -newkey rsa:3072 -keyout file2.pem
Enter PEM pass phrase: **********
Verifying - Enter PEM pass phrase: **********
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:California
Locality Name (eg, city) []:Sunnyvale
Organization Name (eg, company) [Internet Widgits Pty Ltd]:example.com
Organizational Unit Name (eg, section) []:Infrastructure
Common Name (e.g. server FQDN or YOUR name) []:radius.example.com
What is one guideline for continuing to obtain a certificate?
A. You should use a third-party tool to encrypt file2.pem before sending it and file1.pem to the CA.

B. You should concatenate file1.pem and file2.pem into a single file, and submit that to the desired CA to sign.
C. You should submit file1.pem, but not file2.pem, to the desired CA to sign.
D. You should submit file2.pem, but not file1.pem, to the desired CA to sign.
Answer: C (LEAVE A REPLY)
When using OpenSSL to obtain a certificate signed by a Certification Authority (CA), you should submit the Certificate Signing Request (CSR) file, which is file1.pem, to the CA. The CSR contains the information about the entity requesting the certificate and the public key, but not the private key, which is in file2.pem.
The CA uses the information in the CSR to create and sign the certificate.
1.CSR Submission: The CSR (file1.pem) includes the public key and the entity information required by the CA to issue a certificate.
2.Private Key Security: The private key (file2.pem) should never be sent to the CA or shared; it remains securely stored on the requestor's server.
3.Certificate Issuance: After the CA signs the CSR, the resulting certificate can be used with the private key to establish secure communications.

NEW QUESTION: 35
Refer to Exhibit:



An HPE Aruba Networking 9x00 gateway is part of an HPE Aruba Networking Central group that has the settings shown in the exhibit. What would cause the gateway to drop traffic as part of its IDPS settings?
A. Its site-to-site VPN connections failing
B. Traffic matching a rule in the active ruleset
C. Its IDPS engine failing
D. Traffic showing anomalous behavior
Answer: B (LEAVE A REPLY)
1. IDPS Mode Configuration Overview

The exhibit shows the HPE Aruba Networking Central settings for the Gateway IDS/IPS configuration:
* Mode: Configured for Intrusion Prevention System (IPS), meaning that the gateway actively blocks traffic identified as threats.
* Fail Strategy: Configured to Block, meaning that if the gateway cannot determine the traffic's nature due to a system issue, it will block the traffic.
* Ruleset: The gateway uses a predefined set of intrusion detection/prevention rules (ruleset version
9861), which is updated automatically every day.
2. Traffic Evaluation in IPS Mode
In IPS mode, the gateway analyzes traffic against the active ruleset:
* If traffic matches a rule in the ruleset and is deemed malicious, the gateway will drop the traffic as part of its prevention mechanism.
* The ruleset defines specific conditions (e.g., signatures of known attacks, protocol anomalies) under which traffic should be blocked.
3. Explanation of Each Option
* A. Its site-to-site VPN connections failing:
* Incorrect:
* Site-to-site VPN connection issues do not directly trigger traffic drops under IDPS settings.
* IDPS is focused on detecting and preventing malicious activity, not general connectivity issues.
* B. Traffic matching a rule in the active ruleset:
* Correct:
* In IPS mode, the gateway drops traffic that matches any predefined rules in the active ruleset.
* For example, if traffic matches the signature of a known exploit or attack, it is immediately blocked.
* C. Its IDPS engine failing:
* Incorrect:
* The fail strategy determines how the gateway behaves in the event of an IDPS engine failure.
* In this case, the fail strategy is set to Block, but this applies only if the engine itself fails, not as a proactive traffic drop mechanism.
* D. Traffic showing anomalous behavior:
* Incorrect:
* While anomalous behavior may be logged or flagged, it does not necessarily lead to traffic drops unless it matches a specific rule in the active ruleset.
* Anomaly detection alone is not sufficient for IPS action without explicit rule matches.
Final Outcome:
Traffic is dropped only when it matches a rule in the active ruleset, ensuring targeted prevention of malicious activity.
References
* Aruba Gateway IDS/IPS Configuration Guide.
* Aruba Central Ruleset Management Documentation.

* Best Practices for Configuring Fail Strategies in IPS Mode.

NEW QUESTION: 36
You are helping an organization deploy HPE Aruba Networking SSE. What is one reason to recommend that the company install agents on remote users' devices?
A. To run posture checks and apply different permissions based on those checks.
B. To permit admins to manage the HPE Aruba Networking SSE policy rules.
C. To permit users to access private servers using SSH.
D. To run threat inspection on clients in a local sandbox rather than in the cloud.
Answer: (SHOW ANSWER)
* Installing Agents for SSE (Secure Service Edge):
* Agents installed on remote users' devices allow posture checks (e.g., antivirus status, OS version) to ensure compliance.
* Based on the results of the posture checks, different permissions and security policies can be applied dynamically.
* This improves the security posture of remote users before granting access to resources.
* Option A: Correct. Agents enable posture checks and enforce conditional access based on compliance.
* Option B: Incorrect. Admins manage SSE policies centrally, not via agents.
* Option C: Incorrect. Access to private servers via SSH does not require agents; it relies on policies and tunnels.
* Option D: Incorrect. Local sandboxing is generally a function of endpoint protection solutions, not SSE agents.

NEW QUESTION: 37
A company wants to implement Virtual Network based Tunneling (VNBT) on a particular group of users and assign those users to an overlay network with VNI
3000.
Assume that an AOS-CX switch is already set up to:
. Implement 802.1X to HPE Aruba Networking ClearPass Policy Manager (CPPM)
. Participate in an EVPN VXLAN solution that includes VNI 3000
Which setting should you configure in the users' AOS-CX role to apply VNBT to them when they connect?
A. Gateway zone set to "3000" with no gateway role set
B. Gateway zone set to "vni-3000" with no gateway role set
C. Access VLAN set to the VLAN mapped to VNI 3000
D. Access VLAN ID set to "3000"
Answer: C (LEAVE A REPLY)
To apply Virtual Network based Tunneling (VNBT) to a particular group of users and assign them to an overlay network with VNI 3000, you should configure the users' AOS-CX role to set the Access VLAN to the VLAN mapped to VNI 3000. This ensures that when users connect, their

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

NEW QUESTION: 38
A company has AOS-CX switches at the access layer, managed by HPE Aruba Networking Central. You have identified suspicious activity on a wired client. You want to analyze the client's traffic with Wireshark, which you have on your management station.
What should you do?
A. Access the client's switch's CLI from your management station. Access the switch shell and run a TCP dump on the client port.
B. Go to the client's switch in HPE Aruba Networking Central. Use the "Security" page to run a packet capture.
C. Set up a policy that implements a captive portal redirect to your management station. Apply that policy to the client's port.
D. Set up a mirror session on the client's switch; set the client port as the source and your station IP address as the tunnel destination.
Answer: (SHOW ANSWER)
Why a Mirror Session Is the Correct Choice
To analyze a wired client's traffic with Wireshark, you need the traffic mirrored to your management station where Wireshark is installed. The most effective way to achieve this is by configuring a mirror session on the AOS-CX switch, specifying the client port as the source and your management station as the destination.
Analysis of Each Option
A: Access the client's switch's CLI from your management station. Access the switch shell and run a TCP dump on the client port:
* Incorrect:
* AOS-CX switches do not natively support packet capture (e.g., tcpdump) directly on the switch CLI.
* This approach is not feasible for capturing and analyzing live client traffic.
B: Go to the client's switch in HPE Aruba Networking Central. Use the "Security" page to run a packet capture:
* Incorrect:
* HPE Aruba Networking Central provides security insights but does not directly support initiating packet captures for detailed analysis.

* Traffic analysis with tools like Wireshark requires local packet capture at the management station.
C: Set up a policy that implements a captive portal redirect to your management station. Apply that policy to the client's port:
* Incorrect:
* Captive portals are designed for user authentication and redirection, not traffic analysis.
* This would disrupt the client's network activity without enabling traffic analysis in Wireshark.
D: Set up a mirror session on the client's switch; set the client port as the source and your station IP address as the tunnel destination:
* Correct:
* Mirroring the client port to your management station is the standard method for analyzing live network traffic with Wireshark.
* Steps include:
* Configure a mirror session on the client's AOS-CX switch.
* Set the client's port as the source.
* Set your management station as the destination using its IP address (via GRE tunnel or physical interface).
* Start capturing traffic with Wireshark on the management station.
Final Recommendation
To analyze the client's traffic, configure a mirror session on the switch, set the client port as the source, and direct the traffic to your management station where Wireshark is running.
References
* AOS-CX Switch Port Mirroring Configuration Guide.
* HPE Aruba Networking Central Monitoring and Troubleshooting Best Practices.
* Wireshark Traffic Analysis and Capture Techniques.

NEW QUESTION: 39
A company has AOS-CX switches. The company wants to make it simpler and faster for admins to detect denial of service (DoS) attacks, such as ping or ARP floods, launched against the switches.
What can you do to support this use case?
A. Deploy an NAE agent on the switches to monitor control plane policing (CoPP).
B. Configure the switches to implement RADIUS accounting to HPE Aruba Networking ClearPass and enable HPE Aruba Networking ClearPass Insight.
C. Implement ARP inspection on all VLANs that support end-user devices.
D. Enabling debugging of security functions on the switches.
Answer: A (LEAVE A REPLY)
Why Monitoring Control Plane Policing (CoPP) with an NAE Agent Is Effective for Detecting DoS Attacks

* Control Plane Policing (CoPP): AOS-CX switches use CoPP to protect the CPU from excessive traffic caused by DoS attacks (e.g., ARP floods, ICMP floods). CoPP enforces rate limits and drops malicious traffic at the control plane level.
* NAE (Network Analytics Engine) Agent:
* The NAE on AOS-CX switches can monitor CoPP counters in real time and trigger alerts if thresholds for certain traffic types (e.g., ICMP, ARP) are exceeded.
* Admins can use NAE to automate detection and respond faster to DoS attacks.
Analysis of Each Option
A: Deploy an NAE agent on the switches to monitor control plane policing (CoPP):
* Correct:
* NAE agents provide real-time visibility into CoPP behavior, helping detect DoS attacks more quickly.
* By analyzing CoPP statistics, the NAE can pinpoint abnormal traffic patterns and alert admins.
* This is the most efficient and scalable solution for this use case.
B: Configure the switches to implement RADIUS accounting to HPE Aruba Networking ClearPass and enable HPE Aruba Networking ClearPass Insight:
* Incorrect:
* While ClearPass can provide visibility into user authentication and device activity, it is not specifically designed to detect or mitigate DoS attacks against switches.
C: Implement ARP inspection on all VLANs that support end-user devices:
* Incorrect:
* ARP inspection helps mitigate ARP spoofing or poisoning, but it does not directly address detection of DoS attacks like ICMP or ARP floods.
* It is a preventative measure, not a detection tool.
D: Enabling debugging of security functions on the switches:
* Incorrect:
* Debugging logs can help troubleshoot specific issues but are not practical for real-time detection of DoS attacks.
* Enabling debugging can overload the switch and is not suitable for proactive monitoring.
Final Recommendation
Deploying an NAE agent to monitor CoPP is the best solution because it provides real-time detection, alerting, and insights into traffic patterns that indicate DoS attacks.
References
* AOS-CX Network Analytics Engine (NAE) Configuration Guide.
* HPE Aruba AOS-CX Control Plane Policing Documentation.
* Best Practices for Protecting Switches Against DoS Attacks in Aruba Networks.

NEW QUESTION: 40
You are setting up an HPE Aruba Networking VIA solution for a company. You have already created a VPN pool with IP addresses for the remote clients. During tests, however, the clients do not receive IP addresses from that pool.

What is one setting to check?
A. That the pool uses valid, public IP addresses that are assigned to the company
B. That the pool is associated with the role to which the VIA clients are being assigned
C. That the pool uses an IP subnet that is different from any subnet configured on the VPNC
D. That the pool is referenced in the clients' VIA Connection Profile
Answer: (SHOW ANSWER)
If VIA clients are not receiving IP addresses from the configured VPN pool, one setting to check is whether the pool is associated with the role to which the VIA clients are being assigned. The association between the IP pool and the role ensures that clients assigned to that role receive IP addresses from the correct pool.
1.Role Association: Each role can be associated with a specific IP pool, ensuring that clients assigned to the role receive addresses from the intended pool.
2.IP Allocation: Proper configuration of the IP pool and its association with the role is crucial for correct IP address allocation.
3.VIA Configuration: Ensuring that all settings, including IP pool associations, are correctly configured, facilitates seamless client connectivity.

NEW QUESTION: 41
A company has a variety of HPE Aruba Networking solutions, including an HPE Aruba Networking infrastructure and HPE Aruba Networking ClearPass Policy Manager (CPPM). The company passes traffic from the corporate LAN destined to the data center through a third-party SRX firewall. The company would like to further protect itself from internal threats. What is one solution that you can recommend?
A. Have the third-party firewall send Syslogs to CPPM, which can work with network devices to lock internal attackers out of the network.
B. Add ClearPass Device Insight (CPDI) to the solution, integrate it with the third-party firewall to develop more complete device profiles.
C. Configure CPPM to poll the third-party firewall for a broad array of information about internal clients, such as profile and posture.
D. Use tunnel mode SSIDs and user-based tunneling (UBT) on AOS-CX switches to pass all internal traffic directly through the third-party firewall.
Answer: A (LEAVE A REPLY)
* Syslog Integration with CPPM:
* ClearPass Policy Manager (CPPM) can integrate with third-party firewalls via Syslog messages to detect and respond to internal threats.
* The Syslog integration enables CPPM to gather context on suspicious activity and enforce appropriate policies such as isolating attackers by working with network devices like Aruba switches and APs.
* Option A: Correct. This method allows for dynamic response to threats and leverages existing infrastructure without requiring major reconfiguration.

* Option B: Incorrect. CPDI is primarily used for profiling devices, not directly for threat response based on Syslog information.
* Option C: Incorrect. While it is possible for CPPM to poll information, this approach is less dynamic and not focused on immediate threat response.
* Option D: Incorrect. Tunnel mode SSIDs and UBT are designed for forwarding user traffic securely but do not directly enhance threat detection or mitigation.

NEW QUESTION: 42
A company is using HPE Aruba Networking ClearPass Device Insight (CPDI) (the standalone application). In the CPDI security settings, Security Analysis is On, the Data Source is ClearPass Devices Insight, and Enable Posture Assessment is On. You see that device has a Risk Score of 90.
What can you know from this information?
A. The posture is unhealthy, and CPDI has also detected at least one vulnerability on the device.
B. The posture is unhealthy, but CPDI has not detected any vulnerabilities on the device.
C. The posture is healthy, but CPDI has detected multiple vulnerabilities on the device.
D. The posture is unknown, and CPDI has detected exactly four vulnerabilities on the device.
Answer: A (LEAVE A REPLY)
In HPE Aruba Networking ClearPass Device Insight (CPDI), a device with a Risk Score of 90 indicates that the posture is unhealthy, and CPDI has detected at least one vulnerability on the device. The risk score is a reflection of the device's security posture and detected vulnerabilities. A high risk score, such as 90, typically signifies significant security concerns, including the presence of vulnerabilities that could be exploited, thereby categorizing the device as a high-risk asset within the network.

NEW QUESTION: 43
HPE Aruba Networking ClearPass Device Insight (CPDI) could not classify some endpoints using system and user rules. Using machine learning, it did assign those endpoints to a cluster and discover a recommendation.
In which of these circumstances does CPDI automatically classify the endpoints based on that recommendation?
A. The recommendation has 96% confidence, and it is based on 13 classified devices.
B. The recommendation has 98% confidence, and it is based on 5 classified devices.
C. The recommendation has 93% confidence, and it is based on 36 classified devices.
D. The recommendation has 100% confidence, and it is based on 4 classified devices.
Answer: (SHOW ANSWER)
Comprehensive Detailed Explanation
HPE Aruba Networking ClearPass Device Insight (CPDI) uses machine learning to assign endpoints to clusters and provide classification recommendations. For CPDI to automatically classify endpoints, specific thresholds of confidence and supporting classified devices must be met.

The generally required thresholds are:
* Minimum Confidence Level: Typically, CPDI requires a recommendation confidence level of at least
95%.
* Minimum Supporting Devices: CPDI needs a cluster to include at least 10 classified devices to ensure the recommendation is statistically meaningful.
Analysis of Each Option:
* A. 96% confidence with 13 classified devices: Meets both thresholds (confidence > 95% and # 10 devices). CPDI will automatically classify endpoints in this scenario.
* B. 98% confidence with 5 classified devices: Confidence level is sufficient, but the cluster lacks the minimum required 10 classified devices. Automatic classification does not occur.
* C. 93% confidence with 36 classified devices: The confidence level is below the required 95%. Automatic classification does not occur.
* D. 100% confidence with 4 classified devices: Confidence is ideal, but there are insufficient supporting classified devices. Automatic classification does not occur.
References
* HPE Aruba ClearPass Device Insight Deployment Guide.
* Aruba ClearPass Machine Learning and Device Classification Thresholds.

NEW QUESTION: 44
What is a use case for the HPE Aruba Networking ClearPass OnGuard dissolvable agent?
A. Continuously monitoring Windows domain clients for compliance
B. Implementing a one-time compliance scan
C. Auto-remediating posture issues on clients
D. Periodically scanning Linux clients for security issues
Answer: B (LEAVE A REPLY)
The use case for the HPE Aruba Networking ClearPass OnGuard dissolvable agent is implementing a one- time compliance scan. The dissolvable agent is designed to perform a compliance check without requiring a permanent installation on the client device. This is ideal for environments where a quick, temporary assessment of the device's security posture is needed without the overhead of a persistent agent.
1.Dissolvable Agent: The dissolvable agent is downloaded and executed on the client device for a single session, performing the necessary compliance checks before being removed automatically.
2.One-time Compliance Scan: This method is particularly useful for guest or unmanaged devices where a temporary compliance scan is sufficient to ensure security standards are met.
3.Minimal Impact: Since the agent does not persist on the client device, it minimizes the impact on the user's system and does not require ongoing maintenance or updates.

NEW QUESTION: 45
A company lacks visibility into the many different types of user and IoT devices deployed in its internal network, making it hard for the security team to address those devices.

Which HPE Aruba Networking solution should you recommend to resolve this issue?
A. HPE Aruba Networking ClearPass Device Insight (CPDI)
B. HPE Aruba Networking Network Analytics Engine (NAE)
C. HPE Aruba Networking Mobility Conductor
D. HPE Aruba Networking ClearPass OnBoard
Answer: A (LEAVE A REPLY)
For a company that lacks visibility into various types of user and IoT devices on its internal network, HPE Aruba Networking ClearPass Device Insight (CPDI) is the recommended solution. CPDI provides comprehensive visibility and profiling of all devices connected to the network. It uses machine learning and AI to identify and classify devices, offering detailed insights into their behavior and characteristics. This enhanced visibility enables the security team to effectively monitor and manage network devices, improving overall network security and compliance.

NEW QUESTION: 46
A company needs to enforce 802.1X authentication for its Windows domain computers to HPE Aruba Networking ClearPass Policy Manager (CPPM). The company needs the computers to authenticate as both machines and users in the same session.
Which authentication method should you set up on CPPM?
A. TEAP
B. PEAP MSCHAPv2
C. EAP-TTLS
D. EAP-TLS
Answer: A (LEAVE A REPLY)
To enforce 802.1X authentication for Windows domain computers to HPE Aruba Networking ClearPass Policy Manager (CPPM) and have the computers authenticate as both machines and users in the same session, you should set up TEAP (Tunneled EAP) as the authentication method. TEAP supports both machine and user authentication within a single 802.1X session, making it suitable for scenarios where both types of authentication are required simultaneously.

NEW QUESTION: 47

A company uses HPE Aruba Networking ClearPass Policy Manager (CPPM) as a TACACS+ server to authenticate managers on its AOS-CX switches. You want to assign managers to groups on the AOS-CX switch by name.
How do you configure this setting in a CPPM TACACS+ enforcement profile?
A. Add the Shell service and set autocmd to the group name.
B. Add the Shell service and set priv-lvl to the group name.
C. Add the Aruba:Common service and set Aruba-Admin-Role to the group name.
D. Add the Aruba:Common service and set Aruba-Priv-Admin-User to the group name.
Answer: (SHOW ANSWER)
To assign managers to groups on the AOS-CX switch by name using HPE Aruba Networking ClearPass Policy Manager (CPPM) as a TACACS+ server, you should add the Aruba service to the TACACS+ enforcement profile and set the Aruba-Admin-Role to the group name. This configuration ensures that the appropriate administrative roles are assigned to managers based on their group membership, allowing for role-based access control on the AOS-CX switches.

NEW QUESTION: 48
You have configured an AOS-CX switch to implement 802.1X on edge ports. Assume ports operate in the default auth-mode. VoIP phones are assigned to the
"voice" role and need to send traffic that is tagged for VLAN 12.
Where should you configure VLAN 12?
A. As the trunk native VLAN on edge ports and the trunk native VLAN on the "voice" role
B. As a trunk allowed VLAN on edge ports and the trunk native VLAN in the "voice" role
C. As the trunk native VLAN in the "voice" role (and not in the edge port settings)
D. As the allowed trunk VLAN in the "voice" role (and not in the edge port settings)
Answer: D (LEAVE A REPLY)
When configuring 802.1X authentication on edge ports of an AOS-CX switch and assigning VoIP phones to a
"voice" role, the correct approach is to configure VLAN 12 as the allowed trunk VLAN in the "voice" role.
This setup ensures that traffic tagged for VLAN 12 is appropriately managed by the role applied to the VoIP phones. In AOS-CX switches, the role-based VLAN configuration allows for more granular control and ensures that the VoIP phones' traffic is handled correctly without altering the edge port settings, which typically operate with default settings for authentication.

NEW QUESTION: 49
What is one benefit of integrating HPE Aruba Networking ClearPass Policy Manager (CPPM) with third-party solutions such as Mobility Device Management (MDM) and firewalls?
A. CPPM can exchange contextual information about clients with third-party solutions, which helps make better decisions.
B. CPPM can make the third-party solutions more secure by adding signature-based threat detection capabilities.

C. CPPM can offload policy decisions to the third-party solutions, enabling CPPM to respond to authentication requests more quickly.
D. CPPM can take over filtering internal traffic so that the third-party solutions have more processing power to devote to filtering external traffic.
Answer: (SHOW ANSWER)
* Contextual Exchange for Better Decisions:
* HPE Aruba ClearPass can integrate with third-party solutions like MDM and firewalls to exchange contextual information about endpoints (e.g., device type, posture, location).
* This integration allows ClearPass and the third-party solutions to make better access control and security decisions.
* For example:
* An MDM can inform CPPM about device compliance, and CPPM can adjust enforcement policies dynamically.
* Firewalls can receive updated context about users and devices to enforce policies more effectively.
* Option Analysis:
* Option A: Correct. Exchanging contextual information improves access control decisions.
* Option B: Incorrect. CPPM does not provide signature-based threat detection.
* Option C: Incorrect. CPPM does not offload policy decisions; it integrates for collaboration.
* Option D: Incorrect. CPPM does not replace third-party traffic filtering capabilities.

NEW QUESTION: 50
A company has a third-party security appliance deployed in its data center. The company wants to pass all traffic for certain clients through that device before forwarding that traffic toward its ultimate destination.
Which AOS-CX switch technology fulfills this use case?
A. Virtual Network Based Tunneling (VNBT)
B. MC-LAG
C. Network Analytics Engine (NAE)
D. Device profiles
Answer: A (LEAVE A REPLY)
Comprehensive Detailed Explanation
Virtual Network Based Tunneling (VNBT) is the appropriate technology for this use case because:
* Traffic Steering: VNBT enables traffic from specific clients or devices to be tunneled through a predefined network path. This allows traffic to pass through intermediate devices such as third-party security appliances.
* Policy Enforcement: VNBT can be configured to route traffic based on roles, VLANs, or other policy definitions, ensuring that only specified traffic flows are redirected to the security appliance.
* Scalability: This approach simplifies the redirection of traffic without requiring complex physical rewiring or changes to the underlying network topology.
Other Options:

* MC-LAG: Primarily used for high-availability and redundancy in multi-chassis link aggregation scenarios, not for traffic redirection through appliances.
* Network Analytics Engine (NAE): Used for monitoring and analytics, not traffic steering or forwarding.
* Device Profiles: Helps automate switch port configurations for specific device types but does not handle traffic redirection.
References
* AOS-CX Virtual Network Based Tunneling (VNBT) documentation.
* Aruba Switch Architecture and Traffic Flow Control Best Practices Guide.

NEW QUESTION: 51
A company has HPE Aruba Networking gateways that implement gateway IDS/IPS. Admins sometimes check the Security Dashboard, but they want a faster way to discover if a gateway starts detecting threats in traffic.
What should they do?
A. Integrate HPE Aruba Networking ClearPass Device Insight (CPDI) with Central and schedule hourly reports.
B. Set up Webhooks that are attached to the HPE Aruba Networking Central Threat Dashboard.
C. Set up email notifications using HPE Aruba Networking Central's global alert settings.
D. Use Syslog to integrate the gateways with HPE Aruba Networking ClearPass Policy Manager (CPPM) event processing.
Answer: (SHOW ANSWER)

NEW QUESTION: 52
A company has HPE Aruba Networking APs (AOS-10), which authenticate clients to HPE Aruba Networking ClearPass Policy Manager (CPPM). CPPM is set up to receive a variety of information about clients' profile and posture. New information can mean that CPPM should change a client's enforcement profile.
What should you set up on the APs to help the solution function correctly?
A. In the security settings, configure dynamic denylisting.
B. In the RADIUS server settings for CPPM, enable Dynamic Authorization.
C. In the WLAN profiles, enable interim RADIUS accounting.
D. In the RADIUS server settings for CPPM, enable querying the authentication status.
Answer: B (LEAVE A REPLY)
To ensure that HPE Aruba Networking APs (AOS-10) properly interact with HPE Aruba Networking ClearPass Policy Manager (CPPM) and dynamically update a client's enforcement profile based on new profile and posture information, you should enable Dynamic Authorization in the RADIUS server settings for CPPM. This allows ClearPass to send Change of Authorization (CoA) requests to the APs, prompting them to reapply the appropriate enforcement profiles based on updated information.

1.Dynamic Authorization: Enabling this feature allows ClearPass to dynamically push changes to the APs whenever there is new relevant information about a client's profile or posture.
2.Change of Authorization (CoA): This mechanism ensures that clients are assigned the correct enforcement profiles in real-time, based on the latest data.
3.Enhanced Policy Enforcement: This setup helps in maintaining accurate and up-to-date policy enforcement for clients on the network.

NEW QUESTION: 53
A company is implementing HPE Aruba Networking Wireless IDS/IPS (WIDS/WIPS) on its AOS-10 APs, which are managed in HPE Aruba Networking Central.
What is one requirement for enabling detection of rogue APs?
A. Each VLAN in the network assigned on at least one AP's or AM's port
B. A Foundation with Security license for each of the APs
C. One AM deployed for every one AP deployed
D. A manual radio profile that enables non-regulatory channels
Answer: B (LEAVE A REPLY)
To enable the detection of rogue APs with HPE Aruba Networking Wireless IDS/IPS (WIDS/WIPS) on AOS-
10 APs managed in HPE Aruba Networking Central, each AP must have a Foundation with Security license.
This license enables advanced security features, including rogue AP detection, which is crucial for maintaining a secure wireless environment and protecting against unauthorized access points.

NEW QUESTION: 54
A company needs you to integrate HPE Aruba Networking ClearPass Policy Manager (CPPM) with HPE Aruba Networking ClearPass Device Insight (CPDI). What is one task you should do to prepare?
A. Install the root CA for CPPM's HTTPS certificate as trusted in the CPDI application.
B. Enable Insight in the CPPM server configuration settings.
C. Configure WMI, SSH, and SNMP external accounts for device scanning on CPPM.
D. Collect a Data Collector token from HPE Aruba Networking Central.
Answer: B (LEAVE A REPLY)
* ClearPass Device Insight Integration:
* To integrate ClearPass Device Insight (CPDI) with ClearPass Policy Manager (CPPM), you must enable the Insight feature in the CPPM server configuration settings.
* This ensures CPPM can share and receive profiling data with CPDI for device identification.
* Option Analysis:
* Option A: Incorrect. Root CA certificates are not required for this integration.
* Option B: Correct. Enabling Insight on CPPM is essential for the integration to function.
* Option C: Incorrect. WMI, SSH, and SNMP are not part of the CPDI integration prerequisites.
* Option D: Incorrect. The Data Collector token is relevant to Aruba Central, not CPDI integration.

NEW QUESTION: 55
A company uses HPE Aruba Networking ClearPass Policy Manager (CPPM) as a TACACS+ server to authenticate managers on its AOS-CX switches. The company wants CPPM to control which commands managers are allowed to enter. You see there is no field to enter these commands in ClearPass.
How do you start configuring the command list on CPPM?
A. Add the Shell service to the managers' TACACS+ enforcement profiles.
B. Edit the TACACS+ settings in the AOS-CX switches' network device entries.
C. Create an enforcement policy with the TACACS+ type.
D. Edit the settings for CPPM's default TACACS+ admin roles.
Answer: A (LEAVE A REPLY)
To control which commands managers are allowed to enter on AOS-CX switches using HPE Aruba Networking ClearPass Policy Manager (CPPM) as a TACACS+ server, you need to add the Shell service to the TACACS+ enforcement profiles for the managers. This service allows you to define and enforce specific command sets and access privileges for users authenticated via TACACS+. By configuring the Shell service in the enforcement profile, you can specify the commands that are permitted or denied for the managers, ensuring controlled and secure access to the switch's command-line interface.

NEW QUESTION: 56
You need to create a rule in an HPE Aruba Networking ClearPass Policy Manager (CPPM) role mapping policy that references a ClearPass Device Insight Tag.
Which Type (namespace) should you specify for the rule?
A. Application
B. Tips
C. Device
D. Endpoint
Answer: D (LEAVE A REPLY)
When creating a rule in an HPE Aruba Networking ClearPass Policy Manager (CPPM) role mapping policy that references a ClearPass Device Insight Tag, you should specify the "Endpoint" Type (namespace) for the rule. This ensures that the policy can properly reference and utilize the tags assigned to endpoints by ClearPass Device Insight for making role mapping decisions.
1.Endpoint Tags: ClearPass Device Insight assigns tags to endpoints based on their characteristics and behaviors. These tags are stored in the "Endpoint" namespace.
2.Role Mapping: By referencing the "Endpoint" type, the rule can accurately match endpoints with the specified tags and apply the appropriate role mappings based on the device's profile.
3.Policy Consistency: Ensuring that the correct namespace is used maintains consistency and accuracy in role assignment policies.

NEW QUESTION: 57
You need to set up HPE Aruba Networking ClearPass Policy Manager (CPPM) to provide certificate- based authentication of 802.1X supplicants. How should you upload the root CA certificate for the supplicants' certificates?
A. As a ClearPass Server certificate with the RADIUS/EAP usage.
B. As a ClearPass Server certificate with the Database usage.
C. As a Trusted CA with the AD/LDAP usage.
D. As a Trusted CA with the EAP usage.
Answer: D (LEAVE A REPLY)
* 802.1X Authentication Workflow: Requires the root CA certificate of the issuing authority for the supplicants' certificates. This ensures that the server can validate the client certificate during the EAP- TLS handshake.
* Trusted CA Usage: In ClearPass, certificates with "Trusted CA" usage are used for validating client and server identities during secure authentication exchanges.
* Option A: Incorrect. The "ClearPass Server certificate" is used for server-side identity verification and is not used to validate client certificates.
* Option B: Incorrect. Database usage is unrelated to RADIUS/EAP or certificate validation.
* Option C: Incorrect. While LDAP/AD integration supports certificate validation, this is not the primary purpose of Trusted CAs for 802.1X.
* Option D: Correct. Trusted CAs for EAP are required to validate client certificates during the authentication process.
By uploading the root CA as a "Trusted CA with EAP usage," the CPPM can properly authenticate the certificates presented by the supplicants during EAP-TLS negotiations.

NEW QUESTION: 58
Your company wants to implement Tunneled EAP (TEAP).
How can you set up HPE Aruba Networking ClearPass Policy Manager (CPPM) to enforce certificated-based authentication for clients using TEAP?
A. For the service using TEAP, set the authentication source to an internal database.
B. Select a service certificate when you specify TEAP as a service's authentication method.
C. Create an authentication method named "TEAP" with the type set to EAP-TLS.
D. Select an EAP-TLS-type authentication method for the TEAP method's inner method.
Answer: D (LEAVE A REPLY)
To set up HPE Aruba Networking ClearPass Policy Manager (CPPM) to enforce certificate-based authentication for clients using Tunneled EAP (TEAP), you need to select an EAP-TLS-type authentication method for TEAP's inner method. TEAP allows for a combination of certificate-based (EAP-TLS) and password-based (EAP-MSCHAPv2) authentication. By choosing EAP-TLS as the inner method, you ensure that the clients are authenticated using their certificates, thus enforcing certificate-based authentication within the TEAP framework.

NEW QUESTION: 59

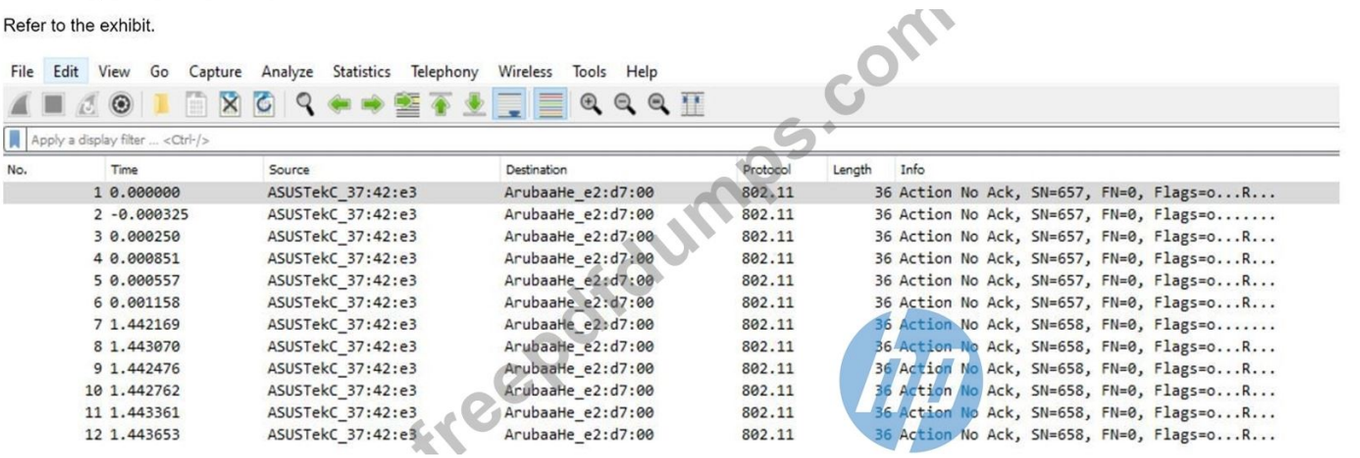
A company has AOS-CX switches and HPE Aruba Networking ClearPass Policy Manager (CPPM).
The company wants switches to implement 802.1X authentication to CPPM and download user roles.
What is one task that you must complete on CPPM to support this use case?
A. Export roles on CPPM to a file that uses XML format.
B. Create an admin account for the switch on CPPM with the HPE Aruba Networking User Role Download privilege level.
C. Configure RADIUS enforcement profiles that specify the HPE-User-Role VSA.
D. Upload the switch TPM certificate as a trusted CA certificate with the Others usage.
Answer: C (LEAVE A REPLY)
* 802.1X and User Role Download:
* AOS-CX switches use RADIUS attributes to dynamically download user roles from CPPM.
* The HPE-User-Role VSA (Vendor-Specific Attribute) must be configured in the RADIUS enforcement profiles to specify which role the switch should apply.
* Option Analysis:
* Option A: Incorrect. Exporting roles in XML is not needed for dynamic role download.
* Option B: Incorrect. Switches authenticate via RADIUS, not admin accounts with specific privileges.
* Option C: Correct. RADIUS enforcement profiles must include the HPE-User-Role VSA to implement user role download.
* Option D: Incorrect. TPM certificates are unrelated to RADIUS-based user role downloads.

NEW QUESTION: 60
An AOS-CX switch has this admin user account configured on it:
netadmin in the operators group.
You have configured these commands on an AOS-CX switch:
tacacs-server host cp.example.com key plaintext &12xl,powmay7855
aaa authentication login ssh group tacacs local
aaa authentication allow-fail-through
A user accesses the switch with SSH and logs in as netadmin with the correct password. When the switch sends a TACACS+ request to the ClearPass server at cp.example.com, the server does not send a response.
Authentication times out.
What happens?
A. The user is logged in and granted operator access.
B. The user is logged in and allowed to enter auditor commands only.
C. The user is logged in and granted administrators access.
D. The user is not allowed to log in.
Answer: A (LEAVE A REPLY)
Comprehensive Detailed Explanation

The configuration includes the command aaa authentication allow-fail-through, which specifies that if the TACACS+ server fails to respond (e.g., times out), the switch will proceed to the next authentication method in the sequence, which is local. In this scenario:
* The switch first attempts to authenticate the user against the TACACS+ server.
* When the TACACS+ server fails to respond, the switch falls back to local authentication.
* The user netadmin is a local account configured on the switch and belongs to the operators group.
* As a result, the user is successfully authenticated locally and is granted operator level access.
References
* Aruba AOS-CX User Guide: Authentication fallback mechanisms.
* TACACS+ fallback behavior for HPE Aruba switches.

NEW QUESTION: 61

Refer to the exhibit.



You have downloaded a packet capture that you generated on HPE Aruba Networking Central. When you open the capture in Wireshark, you see the output shown in the exhibit.
What should you do in Wireshark so that you can better interpret the packets?
A. Choose to decode UDP port 5555 packets as ARUBA_ERM and set the Aruba ERM Type to 0.
B. Edit preferences for IEEE 802.11 and chose to ignore the Protection bit with IV.
C. Apply the following display filter: wlan.fc.type == 1.
D. Edit the Enabled Protocols and make sure that 802.11, GRE, and Aruba_ERM are enabled.
Answer: A (LEAVE A REPLY)
To better interpret the packets shown in the Wireshark capture, you should choose to decode UDP port 5555 packets as ARUBA_ERM and set the Aruba ERM Type to 0. This configuration will allow Wireshark to properly decode and display the Aruba-specific encapsulated remote mirroring (ERM) packets, providing a clearer understanding of the traffic.
1.Decoding Protocols: Selecting the correct protocol decoding in Wireshark ensures that the captured packets are interpreted correctly, displaying the relevant information.
2.Aruba ERM: The packets in the capture are likely encapsulated remote mirroring (ERM) packets specific to Aruba, which require proper decoding settings in Wireshark.
3.Clear Interpretation: By setting the Aruba ERM Type to 0 and decoding the packets as ARUBA_ERM, you can view the encapsulated data accurately.

NEW QUESTION: 62
A ClearPass Policy Manager (CPPM) service includes these settings:
* Role Mapping Policy:
* Evaluate: Select first
* Rule 1 conditions:
* Authorization:AD:Groups EQUALS Managers
* Authentication:TEAP-Method-1-Status EQUALS Success
* Rule 1 role: manager
Rule 2 conditions:
* Authentication:TEAP-Method-1-Status EQUALS Success
* Rule 2 role: domain-comp
Default role: [Other]
Enforcement Policy:
* Evaluate: Select first
* Rule 1 conditions:
* Tips Role EQUALS manager AND Tips Role EQUALS domain-comp
* Rule 1 profile list: domain-manager
Rule 2 conditions:
* Tips Role EQUALS manager
* Rule 2 profile list: manager-only
Rule 3 conditions:
* Tips Role EQUALS domain-comp
* Rule 3 profile list: domain-only
Default profile: [Deny access]
A client is authenticated by the service. CPPM collects attributes indicating that the user is in the Contractors group, and the client passed both TEAP methods.
Which enforcement policy will be applied?
A. [Deny Access Profile]
B. manager-only
C. domain-manager
D. domain-only

Answer: (SHOW ANSWER)

1. Understanding the Role Mapping Evaluation:

* Role mapping is set to "Evaluate: Select first," meaning the first rule that matches the client attributes will determine the role(s) assigned.
* Contractors group: Since the client is in the Contractors group (not Managers), Rule 1 in the Role Mapping Policy does not match.
* TEAP-Method-1-Status EQUALS Success: This condition matches Rule 2, so the client is assigned the domain-comp role.
* No other rules match, so the default role [Other] is not applied.

2. Resulting Role from Role Mapping Policy:

* The client is assigned the domain-comp role.

3. Enforcement Policy Evaluation:

* Enforcement policy is also set to "Evaluate: Select first," so the first matching rule determines the enforcement profile.
* Rule 1 (Tips Role = manager AND domain-comp):
* The client only has the domain-comp role, not manager, so this rule does not match.
* Rule 2 (Tips Role = manager):
* The client does not have the manager role, so this rule does not match.
* Rule 3 (Tips Role = domain-comp):
* This rule matches the client's role, but it is not evaluated because the enforcement policy already skipped to the default action after failing the first two rules.

4. Default Enforcement Profile:

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

Final Outcome:

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

References

* Aruba ClearPass Policy Manager Role Mapping and Enforcement Policies Guide.
* Role and Policy Evaluation Logic for ClearPass Authentication Services.