HP.HPE6-A88.v2026-08-11.q124

Exam Code:	HPE6-A88
Exam Name:	HPE Aruba Networking ClearPass Exam
Certification Provider:	HP
Free Question Number:	124
Version:	v2026-08-11
# of views:	137
# of Questions views:	1240
https://www.exam-tests.com/HPE6-A88-exam/HP.HPE6-A88.v2026-08-11.q124.html	

NEW QUESTION: 1
After a guest user submits their self-registration form, their account is created in a disabled state.
What visual cue indicates this status on the registration receipt?
A. The page redirects to the home screen.
B. A warning message is displayed.
C. The Log In button is grayed out.
Answer: C (LEAVE A REPLY)
When a guest account is created in a disabled state, ClearPass visually indicates this on the registration receipt by displaying the Log In button in a grayed-out state, showing that access is not yet permitted until the account is enabled or approved.

NEW QUESTION: 2
An IT administrator needs to ensure that guest receipts for registrations are sent through both email and SMS simultaneously. They have already configured the email relay. What additional step must they take to meet this need?
A. Set up an external SMTP server to handle both email and SMS notifications.
B. Configure the SMS Gateway under ClearPass Guest by clicking the Configure SMS Gateway link in the Messaging Setup window.
C. Enable the dual messaging feature in the ClearPass security settings.
Answer: (SHOW ANSWER)
To send guest receipts through both email and SMS, the administrator must configure the SMS Gateway in ClearPass Guest by selecting "Configure SMS Gateway" in the Messaging Setup window. This enables ClearPass to deliver notifications via both communication channels simultaneously.

NEW QUESTION: 3

An IT administrator attempts to join a ClearPass server to an Active Directory domain. They notice that the system clocks of the ClearPass server and the AD domain are not in sync. The ClearPass server is 10 minutes behind the AD domain. As a best practice, what should the administrator do?

A. The administrator should manually set the ClearPass server clock to match the AD domain.

B. The administrator should sync the ClearPass server and the AD domain to the same time source.

C. The administrator should proceed with the join.

Answer: B (LEAVE A REPLY)

Active Directory authentication relies on Kerberos, which is highly sensitive to time differences.

Synchronizing both the ClearPass server and the Active Directory domain to the same reliable time source ensures proper Kerberos operation and prevents authentication and domain join failures.

NEW QUESTION: 4

Which two protocols can ClearPass use for device posture assessments?

(Choose two)

Response:

A. RADIUS

B. SNMP

C. HTTPS

D. HTTP

Answer: (SHOW ANSWER)

NEW QUESTION: 5

A network administrator is troubleshooting an issue where endpoints are not receiving updated enforcement decisions after a second authentication. What is the most likely configuration change needed?

A. Disable the "Use Cached Results" on enforcement tab.

B. Disable endpoint re-authentication.

C. Increase the frequency of the posture checks.

Answer: A (LEAVE A REPLY)

The most likely fix is to disable the "Use Cached Results" option on the Enforcement tab. When caching is enabled, ClearPass may reuse previous enforcement decisions, preventing updated policies from being applied after re-authentication. Disabling this ensures that each authentication request is freshly evaluated against current posture and policy data.

NEW QUESTION: 6

Where can a ClearPass admin configure sponsor approval workflows for guest registration?
Response:
A. Under OnGuard health settings
B. Inside the Guest module workflow editor
C. In the Role Mapping policy
D. In Insight dashboard
Answer: B (LEAVE A REPLY)

NEW QUESTION: 7
An organization is setting up a ClearPass server for their network authentication. The administrator has installed a certificate issued by an internal Certificate Authority. The clients cannot fully validate the server's certificate during the validation process. What additional step must the administrator take to ensure the clients can successfully validate the certificate?
A. Disable the trust check in the client's validation process.
B. Install the root certificate from the internal Certificate Authority on all client devices.
C. Reissue the certificate from a public Certificate Authority.
Answer: B (LEAVE A REPLY)
For clients to successfully validate a server certificate issued by an internal Certificate Authority, they must trust that CA. Installing the root certificate on all client devices establishes the trust chain, allowing clients to verify the ClearPass server certificate during authentication.

NEW QUESTION: 8
What two factors should be monitored regularly to ensure high availability and performance in ClearPass?
(Choose two)
Response:
A. Guest session timeouts
B. Number of active OnGuard licenses
C. Disk usage and CPU load
D. Authentication latency
Answer: (SHOW ANSWER)

NEW QUESTION: 9
In a corporate network secured with 802.1X authentication, a client device initially receives a quarantine role due to an unknown posture token. After the client completes a health check using the dissolvable OnGuard agent, the health information is processed by the WEBAUTH service.

How does ClearPass utilize this information during the client's second authentication attempt?
A. ClearPass automatically assigns the client to a guest VLAN without further validation.
B. ClearPass references the cached posture token to determine the appropriate enforcement policy.
C. ClearPass requires the client to complete another health check before allowing network access.
Answer: (SHOW ANSWER)
After the health check is completed, ClearPass stores the resulting posture token. During the subsequent 802.1X authentication, ClearPass retrieves this cached posture token and uses it to evaluate posture compliance and apply the correct enforcement policy without requiring the health check to be repeated.

NEW QUESTION: 10
A security analyst needs to ensure that ClearPass sends a notification whenever a report is ready. They want to receive these notifications via SMS. What is the correct procedure to set this up?
A. Set up an email relay and configure it to forward the emails as SMS messages.
B. Configure the SMS Gateway under ClearPass Guest and ensure report notifications are enabled in Insight.
C. Enable SMS notifications in the Administration > External Servers > Messaging Setup menu.
Answer: B (LEAVE A REPLY)
ClearPass uses the SMS Gateway configuration within ClearPass Guest to send SMS messages.
By configuring the SMS Gateway and enabling SMS notifications for reports in Insight, ClearPass can automatically notify the analyst via SMS when a report is ready.

NEW QUESTION: 11
An IT professional decides to configure RADIUS Start/Stop Accounting but not RADIUS Interim accounting.
What is the likely outcome?
A. The Policy Manager will continuously display license limit exceeded messages.
B. The network will efficiently monitor client activity without excessive resource usage.
C. The network will fail to register any client traffic, leading to connectivity issues.
Answer: B (LEAVE A REPLY)
Interim Accounting sends updates to ClearPass every few minutes regarding how much data a client has used. While useful for billing, it generates significant traffic and CPU load in large environments. By using only Start/Stop messages, ClearPass still knows exactly when a user connects and disconnects (which is sufficient for managing session-based

licenses), but the system avoids the overhead of constant updates, leading to more efficient resource usage.

NEW QUESTION: 12
What is the main purpose of the ClearPass Policy Manager?
A. To provide a centralized point for policy enforcement
B. To configure Aruba wireless access points
C. To manage user traffic on the network
D. To optimize the routing protocols in the network
Answer: A (LEAVE A REPLY)
ClearPass Policy Manager allows administrators to create and enforce policies regarding user and device access to the network.

NEW QUESTION: 13
A security admin wants to implement ClearPass to control access for wired and wireless users across multiple campuses. The solution must assign VLANs dynamically, enforce health checks, and restrict access based on user roles. Which three ClearPass features help meet these requirements?
(Choose three)
Response:
A. Device Insight
B. Policy Manager
C. Onboard
D. Role Mapping
E. OnGuard
Answer: B,D,E (LEAVE A REPLY)

NEW QUESTION: 14
When managing network access through ClearPass, an administrator notices that client status changes are causing repeated disconnections and re-authentications. The administrator wants to prevent the service from making the same enforcement decision without considering newly gathered information. What action should the administrator take?
A. Enable automatic endpoint reconciliation.
B. Increase the timeout period for client re-authentication.
C. Select the option 'Use Cached Results' on the enforcement tab.
Answer: A (LEAVE A REPLY)
Enabling automatic endpoint reconciliation ensures that ClearPass updates endpoint attributes dynamically as new information is gathered. This prevents repeated disconnections and redundant enforcement decisions by allowing ClearPass to adapt to the latest endpoint context without reapplying identical policies unnecessarily.

NEW QUESTION: 15
A company uses ClearPass with Active Directory as both the authentication and authorization source. What is the advantage of this setup?
A. It allows for both credential validation and account attribute retrieval.
B. It simplifies the network topology by eliminating external servers.
C. It ensures that only internal devices can access the network.
Answer: A (LEAVE A REPLY)
Using Active Directory for both authentication and authorization allows ClearPass to validate user credentials and simultaneously retrieve directory attributes such as group membership. This enables consistent, attribute-based policy decisions without requiring a separate identity source.

NEW QUESTION: 16
Which two factors are considered when selecting a ClearPass service during policy evaluation?
(Choose two)
Response:
A. IP address of endpoint
B. Authentication source
C. Connection protocol (e.g., EAP, PAP)
D. Endpoint's DNS record
Answer: B,C (LEAVE A REPLY)

NEW QUESTION: 17
Which two types of credentials can be used in ClearPass for authenticating users?
(Choose two)
Response:
A. Username and Password
B. Biometrics
C. Digital Certificates
D. MAC Address

Answer: (SHOW ANSWER)

NEW QUESTION: 18
An IT administrator is setting up a captive portal for a company's network and needs to ensure that the SSL certificate is compatible with the Aruba Instant device they are using. Which type of certificate should the administrator install to meet this requirement?
A. CER certificate
B. PEM certificate
C. DER certificate
Answer: B (LEAVE A REPLY)
The PEM certificate format is required for Aruba Instant devices when configuring SSL on a captive portal. PEM files contain the base64-encoded certificate and private key, making them compatible with Aruba devices for secure HTTPS communication during guest authentication.

NEW QUESTION: 19
An organization wants to ensure that all devices accessing their network meet specific security criteria. They decide to use ClearPass OnGuard to monitor and enforce compliance. Which aspect of ClearPass OnGuard provides this functionality?
A. Network access control
B. Health Checks
C. Security policies
Answer: B (LEAVE A REPLY)
Comprehensive and Detailed Explanation From HPE Aruba Networking ClearPass portfolio:
Health Checks are the core mechanism of OnGuard. These checks look for specific attributes on the endpoint, such as whether the antivirus is up-to-date, if the OS firewall is enabled, or if unauthorized applications (like peer-to-peer software) are running. The result of these checks is a "Posture Token" (Healthy, Unhealthy, or Unknown) that ClearPass uses to make enforcement decisions.

NEW QUESTION: 20
Which authentication method is most secure for 802.1X-based enterprise wireless networks?
Response:
A. EAP-TLS
B. Web-based Captive Portal
C. Open Authentication
D. MAC Authentication
Answer: A (LEAVE A REPLY)

NEW QUESTION: 21
A network administrator notices that a client device leaves the network and returns after ten minutes. Upon reconnecting, the device's posture token is unknown. What is the most likely reason for this behavior?
A. The agent failed to send any updates to ClearPass during the ten-minute period.
B. The posture token expired due to inactivity beyond the five-minute threshold.
C. The endpoint profile information was permanently deleted from ClearPass.
Answer: B (LEAVE A REPLY)
Posture tokens are temporary and have a configurable expiry timer (often defaulted to 5 minutes). If a device disconnects and remains inactive for longer than this threshold, ClearPass clears the token to ensure it doesn't grant access based on potentially stale health data. When the device returns after 10 minutes, it must perform a new health check to regain its "Healthy" status.

NEW QUESTION: 22
Which protocol is most commonly used by ClearPass for Authentication and Authorization tasks?
Response:
A. HTTP
B. NTP
C. SNMP
D. RADIUS
Answer: D (LEAVE A REPLY)

NEW QUESTION: 23
An IT administrator is tasked with creating a self-service portal for guest users to request and maintain their own user identities. Which type of web page should they create using ClearPass Guest's Web Content Manager?
A. Web Logins
B. Self-Registrations
C. Web Pages
Answer: B (LEAVE A REPLY)
Self-Registration pages allow guest users to create, manage, and maintain their own user identities through a self-service portal. ClearPass Guest's Web Content Manager provides this page type specifically for guest-driven account creation and lifecycle management.

NEW QUESTION: 24
Which two methods are commonly used by ClearPass to discover and profile endpoints? (Choose two)
Response:
A. NTP time requests

B. DHCP fingerprinting
C. SQL queries
D. SNMP polling
Answer: (SHOW ANSWER)

NEW QUESTION: 25
An IT specialist is trying to create a reliable profile for a new endpoint device using ClearPass. They want to ensure the profiling is as accurate as possible. What approach should they take?
A. Interface multiple profiling collectors between the client device and ClearPass.
B. Only the HTTP network function is used to detect device fingerprints.
C. Rely solely on the DHCP network function for profiling.
Answer: (SHOW ANSWER)
Accuracy in profiling is cumulative. Relying solely on one method (like DHCP) can result in "Generic" profiles. By enabling multiple collectors -such as DHCP (for OS discovery), HTTP (for browser/version info), and SNMP (for system description/OID)-ClearPass can correlate data points to provide a 100% certain classification. The more "context" ClearPass receives, the more reliable the final enforcement decision becomes.

NEW QUESTION: 26
An organization uses ClearPass to exchange security and descriptive context with external systems. They want to ensure that the communication is not limited to authentication devices. What feature should they leverage?
A. Set up an external SMS Gateway provider for all notifications.
B. Utilize ClearPass's vast array of REST API and HTTP communications.
C. Configure multiple email relays for different services and reports.
Answer: (SHOW ANSWER)
Beyond traditional RADIUS/TACACS, ClearPass acts as a Context Broker . It uses a robust set of REST APIs and HTTP-based outbound notifications to share data with "non-authentication" systems like SIEMs, Next-Generation Firewalls, and Asset Management databases. This allows the entire security infrastructure to benefit from the rich identity and profiling context that ClearPass gathers, enabling a coordinated response to threats across the entire network.

NEW QUESTION: 27
A network administrator is troubleshooting an issue where a user is unable to log in to the Policy Manager's web interface. The administrator checks the Access Tracker but does not see any relevant logs. What should the administrator do next based on ClearPass's handling of TACACS requests?
A. Create a new TACACS service in the Policy Manager.
B. Check the Event Viewer for the TACACS request.

C. Restart the ClearPass server to reset the logs.
Answer: B (LEAVE A REPLY)
While RADIUS requests (for network access) are almost always found in the Access Tracker, TACACS+ requests (for device administration) that fail early in the process-such as those from an unauthorized source IP-may not appear there. In these cases, the Event Viewer is the correct diagnostic tool. The Event Viewer captures system-level errors, including "Unknown NAD" alerts for TACACS+ attempts, which will help the administrator identify why the request isn't being processed by a service.

NEW QUESTION: 28
What is the primary function of the Authentication component in AAA?
Response:
A. Logs session time and data usage
B. Determines what resources a user can access
C. Provides real-time analytics for user activity
D. Confirms the identity of a user or device
Answer: D (LEAVE A REPLY)

NEW QUESTION: 29
In an enterprise environment, a network administrator is tasked with configuring ClearPass to interact with various network access devices (NADs). The administrator needs to ensure that only specific devices can send authentication requests to ClearPass. After navigating to the 'Devices' section under the 'Network' menu, what critical step must the administrator take to add a new NAD to ClearPass properly?
A. Set up a VPN tunnel between the NAD and ClearPass.
B. Configure the device's MAC address in the Add Device window.
C. Enter a source IP address or address range for the device.
Answer: C (LEAVE A REPLY)
When adding a new Network Access Device (NAD) in ClearPass, the administrator must enter the device's source IP address or IP range. This ensures that only authentication requests originating from trusted NADs are accepted by ClearPass, providing controlled and secure communication between the NADs and the authentication server.

NEW QUESTION: 30
Which two protocols are commonly used for Authentication in AAA frameworks?
(Choose two)
Response:
A. SNMP
B. DHCP
C. RADIUS
D. TACACS+

Answer: C,D (LEAVE A REPLY)

NEW QUESTION: 31
An organization uses ClearPass to manage network access for its devices. A device reported as stolen is detected attempting to connect to the network. What action can the EMM server trigger upon receiving an HTTP API call from ClearPass?
A. The EMM server can automatically block all network traffic from the device.
B. The EMM server can send a message to the user or wipe the user's device.
C. The EMM server can permanently disable the device's network interface.
Answer: (SHOW ANSWER)
When ClearPass detects a stolen device and triggers an HTTP API call, the EMM server can take management actions such as notifying the user or remotely wiping the device. These actions are performed by the EMM system based on its device management capabilities and policies.

NEW QUESTION: 32
What is the purpose of the "Service Categorization" feature in ClearPass?
Response:
A. To filter syslog messages
B. To prioritize SNMP responses
C. To map IP addresses to device profiles
D. To classify services for logging and monitoring
Answer: (SHOW ANSWER)

NEW QUESTION: 33
Which ClearPass feature helps manage guest access by providing self-registration?
A. ClearPass Onboard
B. ClearPass Guest
C. ClearPass Profiler
D. ClearPass Policy Manager
Answer: B (LEAVE A REPLY)

ClearPass Guest helps organizations manage guest access, including self-registration for visitors to obtain network access.

NEW QUESTION: 34
A company wants to provide downloadable PDF guides for guests accessing their network. The IT team has uploaded the PDFs to the Content Manager. How should they configure these files to ensure guests can access them via the web server?
A. Store the PDFs in the private files section of the Content Manager.
B. Apply a skin that includes links to the PDFs.
C. Store the PDFs in the public files section of the Content Manager.
Answer: C (LEAVE A REPLY)
The PDFs should be stored in the public files section of the Content Manager so they can be accessed directly via the ClearPass web server by guest users. Public files are available without authentication, making them ideal for downloadable resources such as guides or instructions.

NEW QUESTION: 35
An IT administrator is setting up guest access on a corporate network using ClearPass. They have configured the RADIUS service correctly and enabled the Allow All MAC AUTH method.
However, they notice that clients are not redirected to the captive portal for authentication. What is the likely reason for this issue?
A. The guest repository is not properly tagging the endpoints with the necessary information.
B. The MAC caching feature is not enabled for the guest access service.
C. The 'captive portal access' value does not match the user role on the gateway associated with the captive portal.
Answer: C (LEAVE A REPLY)
Captive portal redirection depends on a match between the role returned by ClearPass and the user role configured on the gateway. If the captive portal access value sent by ClearPass does not exactly match the gateway's captive portal role, the gateway will not trigger the redirect, even though MAC authentication is allowed.

NEW QUESTION: 36
A network administrator needs to revoke a certificate for a lost device to ensure it no longer has network access. They navigate to the Certificate Authorities section in ClearPass Onboard. What next step should they take to ensure the certificate is properly revoked and the device is blocked?
A. Select the certificate authority, edit the retention policy to store only metadata, and then revoke the certificate.

B. Select the certificate authority, view the issued certificates, and revoke the specific certificate associated with the lost device.
C. Select the certificate authority, view the trust chain, and manually revoke the certificate from the list.
Answer: (SHOW ANSWER)
The administrator should select the certificate authority, view the issued certificates, and revoke the specific certificate associated with the lost device. This action immediately invalidates the certificate, ensuring that the lost device can no longer authenticate or gain access to the network.

NEW QUESTION: 37
An IT professional is setting up a Pre-Authentication Check using RADIUS. They need to ensure that the same service will authenticate the user to the Network Access Device (NAD). What is a crucial step they must take to configure this correctly?
A. Set up a separate RADIUS server to handle the Pre-Authentication Check.
B. Configure the RADIUS server to process the Pre-Authentication Check and the NAD authentication request.
C. Use a different authentication protocol for the NAD.
Answer: B (LEAVE A REPLY)
In a Pre-Authentication workflow (often used in Captive Portals), ClearPass first checks the user's credentials locally or against an external source before the actual NAD (switch/controller) sends the final RADIUS request. For this to work seamlessly, the same service or logic in ClearPass must be able to handle the initial check and the subsequent NAD request to ensure consistency in role assignment and session tracking.

NEW QUESTION: 38
Which ClearPass component is responsible for performing device profiling?
A. ClearPass Policy Manager
B. ClearPass Onboard
C. ClearPass Profiler
D. ClearPass Guest
Answer: (SHOW ANSWER)
ClearPass Profiler is used to identify and classify devices connected to the network based on various characteristics, such as device type, operating system, and other identifiers.

NEW QUESTION: 39
An IT administrator wants to improve the user experience during the login process by reducing unnecessary redirects and ensuring users receive immediate feedback on credential validity.
Which approach should the administrator implement?
A. Configure the NAD to handle more simultaneous connections.

B. Increase the timeout period for RADIUS communication.
C. Enable the pre-authentication check in the ClearPass login process.
Answer: (SHOW ANSWER)
Pre-authentication checks validate credentials before full authentication processing occurs. This provides immediate feedback to users and avoids unnecessary redirects, resulting in a faster and smoother login experience.

NEW QUESTION: 40
Which of the following is a prerequisite before a ClearPass Service can apply an Enforcement Profile?
Response:
A. The service must define a Web Login Form
B. The user must match a Role Mapping rule
C. The system must be in Publisher-only mode
D. The endpoint must be in a known device repository
Answer: B (LEAVE A REPLY)

NEW QUESTION: 41
Which two enforcement methods can ClearPass apply after successful guest authentication?
(Choose two)
Response:
A. Forcing the endpoint to update its OS
B. Assigning dynamic roles or VLANs
C. Applying downloadable user roles
D. Provisioning SSL VPN access
Answer: B,C (LEAVE A REPLY)

NEW QUESTION: 42
Which protocol does ClearPass use to communicate with network devices for authentication?
A. SNMP
B. RADIUS
C. FTP
D. SMTP
Answer: B (LEAVE A REPLY)
ClearPass uses RADIUS (Remote Authentication Dial-In User Service) for authentication, authorization, and accounting in network access control.

NEW QUESTION: 43

An IT administrator is setting up a new service and wants to ensure that non-compliant end hosts are automatically remediated. Which step should they take next?
A. Select the Audit End-hosts check box and choose to perform an audit always.
B. Select the Add new Posture Server link and configure a new server.
C. Select the Posture Compliance check box, enable auto-remediation, and enter the Remediation URL.
Answer: C (LEAVE A REPLY)
ClearPass OnGuard provides the framework for endpoint health checks. In the service selection rules, enabling Posture Compliance tells ClearPass to look for a health token from the OnGuard agent. By selecting auto-remediation , the administrator allows the system to automatically trigger fixes (like starting a disabled firewall) or redirect the user to a Remediation URL where they can find instructions or software updates needed to become compliant.

NEW QUESTION: 44
What determines which ClearPass service handles a specific authentication request?
Response:
A. The endpoint MAC address
B. The ClearPass cluster node that first receives the request
C. The incoming request's RADIUS NAS-IP and authentication method
D. The firewall rule applied to the request
Answer: C (LEAVE A REPLY)

NEW QUESTION: 45
A network engineer is troubleshooting an issue where a user is receiving unexpected access rights. They decide to use the LDAP browser in ClearPass. What feature of the LDAP browser should they use to determine why the user is getting a certain type of access?
A. Edit the list of pre-built filters to include more attributes.
B. Browse the directory tree and look at the user's attributes.
C. Modify the configuration of the ClearPass User Role in the enforcement profile.
Answer: B (LEAVE A REPLY)
The LDAP browser within ClearPass Policy Manager is a critical diagnostic tool used to verify the actual data stored in an external identity store. Because ClearPass bases its Authorization decisions on specific attributes (such as department, memberOf, or accountStatus), the administrator must ensure those attributes are correctly populated in the directory. By browsing the directory tree and inspecting a specific user object, an engineer can see exactly what attributes ClearPass "sees" during a request, helping identify if a role-mapping failure is due to a missing or incorrect LDAP attribute.

NEW QUESTION: 46

A network administrator notices that a client device leaves the network and returns after ten minutes. Upon reconnecting, the device's posture token is unknown. What is the most likely reason for this behavior?
A. The agent failed to send any updates to ClearPass during the ten-minute period.
B. The posture token expired due to inactivity beyond the five-minute threshold.
C. The endpoint profile information was permanently deleted from ClearPass.
Answer: (SHOW ANSWER)
Posture tokens in ClearPass are time-bound and expire after a defined inactivity period. If the client disconnects longer than the allowed validity window, the token expires and is no longer recognized when the device reconnects, resulting in an unknown posture state.

NEW QUESTION: 47
A facility manager is concerned about the security of their network after discovering that an attacker could potentially replace a wired IP camera with a laptop using the same MAC address.
How does the ClearPass profiler mitigate this risk?
A. By creating separate networks for each type of device to prevent unauthorized access.
B. The network can distinguish between the camera and a spoofed device by comprehensively profiling the real client device type.
C. By automatically blocking any device that attempts to connect with a MAC address already in use.
Answer: B (LEAVE A REPLY)
ClearPass Profiler uses multiple device characteristics beyond the MAC address, such as DHCP fingerprinting, traffic behavior, and protocol usage, to accurately identify the true device type. This comprehensive profiling allows the network to distinguish a legitimate IP camera from a spoofed device attempting to use the same MAC address.

NEW QUESTION: 48
A company is setting up a custom Enforcement Profile for operator logins in ClearPass. They decide to copy an existing operator login profile and modify the value of the admin_privileges attribute. What additional step must they take to properly assign this custom profile to the users?

A. Create a new role in the Admin User Repository and link it to the custom profile.
B. Create an application enforcement policy and modify the rules to include the new custom profile.
C. Assign the custom profile directly to users in the Local User Repository.
Answer: A (LEAVE A REPLY)
Operator access and privileges in ClearPass are controlled through roles defined in the Admin User Repository. After creating a custom operator login enforcement profile, it must be linked to a new or existing admin role so that users assigned to that role receive the defined administrative privileges.

NEW QUESTION: 49
An organization wants to enhance its network security by integrating external systems to provide rich context to its authorization logic. They plan to use ClearPass Policy Manager for this purpose. Which feature of the Policy Manager will be most beneficial for integrating with these external systems?
A. Self-service device onboarding with built-in certificate authority
B. Guest access with extensive customization and sponsor-based approvals
C. Configuring external context servers and context server actions through APIs or HTTP/REST calls
Answer: C (LEAVE A REPLY)
Configuring external context servers and context server actions allows ClearPass Policy Manager to integrate with external systems via APIs or HTTP/REST calls. This enables the exchange of contextual data - such as threat intelligence, device posture, or user behavior - to enhance authorization decisions and strengthen network security.

NEW QUESTION: 50
A network administrator wants to ensure that users see their company's logo when accessing the guest network. They have already uploaded the logo as a JPEG file into the Content Manager.
What is the next step they should take to display this logo on the custom web pages?
A. Enable public access for the uploaded logo file.
B. Apply a skin that includes the uploaded logo to the web pages.
C. Edit the ClearPass Guest configuration to include the logo in the default template.
Answer: B (LEAVE A REPLY)
After uploading the company logo to the Content Manager, the administrator must apply a skin that includes the uploaded logo to the guest web pages. Skins define the visual appearance of ClearPass Guest portals, and applying one with the logo ensures the branding appears consistently across all guest-facing pages.

NEW QUESTION: 51

An IT technician is tasked with ensuring that the Network Access Device's (NAD) trust chain is properly configured on ClearPass. They select RadSec for the network device and observe that the PSK is automatically set to 'radsec'. What critical step should the technician take next to ensure secure communication?

A. Manually override the PSK field with a custom value.

B. Reboot the network device to apply the RadSec configuration.

C. Verify that the NAD's trust chain is trusted on ClearPass.

Answer: C (LEAVE A REPLY)

After selecting RadSec, the technician must verify that the Network Access Device's (NAD) trust chain is trusted on ClearPass. RadSec relies on mutual TLS authentication, and secure communication is only established when ClearPass trusts the NAD's certificate chain. The PSK
'radsec' is a placeholder and not used for TLS-based authentication.

NEW QUESTION: 52

Where in ClearPass can administrators define which posture attributes are checked during an OnGuard health evaluation?

Response:

A. Guest Operator Profile Editor

B. Posture Policies within Health Configuration

C. Access Tracker > Posture Logs

D. Onboard Settings > Certificate Policy

Answer: B (LEAVE A REPLY)

NEW QUESTION: 53

An organization wants to enforce role-based access policies across their entire network to ensure that users have appropriate access privileges regardless of their connection point. How does ClearPass facilitate this requirement?

A. By providing detailed audit logs of all network activity

B. By offering customizable user authentication methods

C. By allowing the creation of individual user roles with associated privileges that applies anywhere on the network

Answer: C (LEAVE A REPLY)

ClearPass decouples security policy from physical location. By using Role-Based Access Control (RBAC) , ClearPass assigns a "Role" (e.g., 'HR' or 'Contractor') during the authentication process. This role is then mapped to network-specific attributes (VLANs, ACLs, or VSAs) that the NAD enforces. Because the policy logic resides in ClearPass, the same user receives the same security privileges whether they connect via a wired port in London or Wi-Fi in New York.

NEW QUESTION: 54

What are two key objectives of implementing Network Access Control with ClearPass? (Choose two)
Response:
A. Assign IP addresses dynamically
B. Enforce role-based access policies
C. Ensure device compliance before granting access
D. Maintain switch configuration backups
Answer: (SHOW ANSWER)

NEW QUESTION: 55
In a corporate network secured with 802.1X authentication, a client device initially receives a quarantine role due to an unknown posture token. After the client completes a health check using the dissolvable OnGuard agent, the health information is processed by the WEBAUTH service. How does ClearPass utilize this information during the client's second authentication attempt?
A. ClearPass automatically assigns the client to a guest VLAN without further validation.
B. ClearPass references the cached posture token to determine the appropriate enforcement policy.
C. ClearPass requires the client to complete another health check before allowing network access.
Answer: B (LEAVE A REPLY)
This follows the standard two-stage authentication flow. The first 802.1X attempt fails posture (Unknown) and results in a quarantine redirect. The user runs the dissolvable agent, which sends health data to a WEBAUTH service. ClearPass saves this status. During the second authentication attempt , the 802.1X service checks the cached posture token associated with that device. Finding it is now "Healthy," ClearPass applies the full-access enforcement policy.

NEW QUESTION: 56
An IT administrator notices that a client endpoint has failed a health check and wants to send a notification that will not only inform the user but also force the client to re-authenticate. Which action should the administrator take?
A. Send a message to disable the network interface.
B. Send a notification to disable the network interface.
C. Send a notification with an action to restart the session.
Answer: C (LEAVE A REPLY)
In OnGuard, you can configure Post-Auth Actions . When a device fails compliance, simply telling the user is often not enough. By choosing an action to "Restart the session," ClearPass sends a RADIUS CoA (Change of Authorization) to the switch or controller, which bounces the user's connection. This forces the device to re-authenticate, at which point the new "Unhealthy" status will trigger a restricted or quarantine policy.

NEW QUESTION: 57
An IT administrator needs to configure multiple profile collectors to gather endpoint context data for a diverse network. What is the primary benefit of using ClearPass for this task?
A. It helps manage devices and their security levels by profiling client devices when they connect to the network.
B. It automatically blocks non-corporate devices.
C. It provides a single security policy for all devices.
Answer: A (LEAVE A REPLY)
The primary benefit of profiling is the transition from "MAC-only" visibility to "Context-aware" visibility. By using multiple collectors (DHCP, SNMP, HTTP, SSH, etc.), ClearPass builds a high-fidelity profile of the endpoint. This allows the administrator to write fine-grained policies-for example, allowing a "Workstation" to access the production server but only allowing an "IoT Camera" to access the NVR. Without this profiling context, the system cannot distinguish between different security levels required for diverse hardware.

NEW QUESTION: 58
A network administrator is configuring a corporate network enforcement policy. The policy includes rules for corporate-issued laptops, MDM-enabled tablets, and personal smart devices. However, the administrator notices that some clients are failing all rules due to a lack of profile data. What should the administrator do to ensure these unprofiled clients can access the profiler collectors and receive a profile using best practices?
A. Add a rule that identifies clients without profiles and assigns them a role allowing limited access to the profiler.
B. Increase the frequency of profile data updates from the endpoint profiler.
C. Set the default enforcement profile to 'Allow Access' for all unprofiled clients.
Answer: A (LEAVE A REPLY)
Best practice for profiling is to never grant full access by default . Instead, the enforcement policy should include a fallback rule for unprofiled devices. This rule assigns a "Limited Access" or "Quarantine" role that allows only DHCP and HTTP traffic. This allows the device to communicate just enough to trigger the profiler collectors (like DHCP fingerprinting), after which the device can be re-authenticated with the correct role.

NEW QUESTION: 59
To enhance the guest login experience, an administrator is configuring the Pre-Authentication Check on an Aruba controller. Where should the administrator edit these settings?
A. In the network policies section of the controller.
B. In the Login Form section of the web login page editor.
C. In the certificate management section of the controller interface.
Answer: B (LEAVE A REPLY)

The Pre-Authentication Check is a feature of the ClearPass Guest web page logic. It is configured within the Web Login editor under the Login Form settings. This feature allows ClearPass to verify the user's credentials locally or against an external source before the user's browser is redirected back to the controller to finish the process, ensuring that only valid attempts reach the network device.

NEW QUESTION: 60
An IT administrator attempts to join a ClearPass server to an Active Directory domain. They notice that the system clocks of the ClearPass server and the AD domain are not in sync. The ClearPass server is 10 minutes behind the AD domain. What will be the likely outcome of this attempt to join the domain?
A. The join will succeed but ClearPass will generate a warning about the clock skew.
B. The join will succeed because ClearPass automatically adjusts the clock skew during the join process.
C. The join will fail because Active Directory only allows a maximum of five minutes of clock skew.
Answer: (SHOW ANSWER)
The domain join will fail because Active Directory enforces a maximum allowable clock skew of five minutes between systems for Kerberos authentication. Since the ClearPass server is 10 minutes behind, the Kerberos ticket validation will fail, preventing the join operation.

NEW QUESTION: 61
A network engineer needs to ensure secure and reliable communication between network devices and the RADIUS server over an unsecured network. Which configuration should they implement?
A. Implement RadSec because it encrypts all RADIUS communication and uses TCP for reliable packet delivery.
B. Use UDP for faster message transport and rely on internal network security.
C. Implement RADIUS with PSK because it is simpler to configure and only encrypts passwords.
Answer: A (LEAVE A REPLY)
Traditional RADIUS (UDP 1812/1813) only encrypts the password attribute; the rest of the packet (including the username) is sent in cleartext. Furthermore, UDP is connectionless and can be unreliable over WAN links.
RadSec solves both issues by wrapping RADIUS in TLS , providing full-packet encryption, and using TCP , which provides guaranteed delivery and better handling of MTU issues/fragmentation across unsecured public networks.

NEW QUESTION: 62
A company wants to prevent corporate devices from accessing the guest network. They configure a ClearPass Entity Update Enforcement action to tag devices as corporate clients. What happens when a tagged device attempts to access the guest network?
A. The enforcement action is ignored, and the device accesses the guest network.
B. The guest access service reads the attribute and denies access to the guest network.
C. The corporate client is redirected to a different network.
Answer: (SHOW ANSWER)
Entity Update allows ClearPass to write custom attributes back to its own Endpoint database. Once a device is tagged as "Corporate," this attribute becomes part of the context available to all services. When that device connects to a "Guest" SSID, the Guest Service can include a rule that checks for the "Corporate" tag; if found, the service uses an Enforcement Policy to return a "Deny Access" profile, successfully segmenting corporate assets from the guest network.

NEW QUESTION: 63
A system administrator needs to ensure that a guest operator can only manage accounts that they create. Which option should be configured in the Operator Profile editor to meet this need?
A. Select the operator's start page
B. Operator Filter to determine the accounts the operator can see
C. Export Configuration option for Administrator
Answer: B (LEAVE A REPLY)
The operator filter in the Operator Profile editor restricts visibility and management scope to specific guest accounts. By configuring this filter, the administrator ensures the guest operator can view and manage only the accounts they personally created.

NEW QUESTION: 64
In Aruba ClearPass, what is a "role mapping" used for?
A. To assign a user role based on device attributes
B. To configure network switches
C. To provide encryption for network traffic
D. To determine the IP address range for users

Answer: A (LEAVE A REPLY)
Role mappings are used to assign roles to users or devices based on their attributes. This helps to enforce network policies for different types of users and devices.

NEW QUESTION: 65
A network administrator is troubleshooting an issue where endpoints are not receiving updated enforcement decisions after a second authentication. What is the most likely configuration change needed?
A. Increase the frequency of the posture checks.
B. Disable endpoint re-authentication.
C. Disable the "Use Cached Results" on enforcement tab.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 66
Which authentication method is typically used after Onboard provisioning is complete and the certificate is installed?
Response:
A. Captive Portal
B. EAP-TLS
C. PAP
D. PEAP-MSCHAPv2
Answer: (SHOW ANSWER)

NEW QUESTION: 67
What is the role of the ClearPass Policy Manager when used in conjunction with Aruba wireless access points?
A. To manage user IP addresses
B. To define access policies for wireless clients
C. To configure SSID settings
D. To manage security updates
Answer: (SHOW ANSWER)
ClearPass Policy Manager integrates with Aruba wireless access points to define and enforce policies for wireless clients.

NEW QUESTION: 68
A network engineer is configuring a policy enforcement service on a wired network to minimize deployment effort. They choose a non-AAA enforcement method. What is the main benefit of this approach?
A. It does not require client configuration and requires minimal configuration on the actual switches.
B. It enables advanced security protocols such as 802.1X.

C. It allows dynamic VLAN assignment based on user roles.

Answer: A (LEAVE A REPLY)

Non-AAA enforcement (often called Web-based authentication or MAC-based profiling without 802.1X) is chosen for ease of deployment. 802.1X is highly secure but requires a "Supplicant" (software) configuration on every client device. By using a non-AAA method, the engineer can secure the network using the device's MAC address and a redirect to a web portal, which works on any device with a browser without needing to touch the client's internal network settings.

NEW QUESTION: 69

A network administrator is setting up ClearPass for a large organization and needs to ensure that user credentials are validated efficiently while also gathering rich context about the users. Which authentication source should the administrator prioritize to meet the need?

A. Active Directory

B. SQL Servers

C. Internal Database

Answer: (SHOW ANSWER)

Active Directory should be prioritized because it allows ClearPass to efficiently validate user credentials and retrieve rich contextual information such as group membership, organizational roles, and user attributes. This enhances both authentication accuracy and policy-based access control.

NEW QUESTION: 70

When configuring the role settings by Mobility Gateway in ClearPass, a network engineer notices that the elements required for the role are reusable. What is the primary benefit of this reusability feature?

A. It provides automatic updates to all roles when one role is changed.

B. It enables the use of default system settings without customization.

C. It allows the engineer to create and apply a single definition to multiple roles, saving time and reducing errors.

Answer: C (LEAVE A REPLY)

The reusability of role elements in ClearPass allows administrators to define a single configuration and apply it across multiple roles. This streamlines setup, reduces configuration time, and minimizes errors by ensuring consistency in role-based access definitions across the network.

NEW QUESTION: 71

An IT administrator notices that a client endpoint has failed a health check and wants to send a notification that will not only inform the user but also force the client to re-authenticate. Which action should the administrator take?

A. Send a message to disable the network interface.
B. Send a notification to disable the network interface.
C. Send a notification with an action to restart the session.
Answer: (SHOW ANSWER)
The administrator should send a notification with an action to restart the session. This forces the client to re-authenticate after failing a health check, allowing ClearPass to reassess the device's compliance status and apply the appropriate enforcement policy based on the updated posture.

NEW QUESTION: 72
Why would an administrator use Downloadable User Roles (DUR) in a ClearPass-Aruba environment?
Response:
A. To simplify AP configuration across sites
B. To enforce access policies dynamically at the network edge
C. To centralize user credentials in ClearPass
D. To monitor active directory group usage
Answer: B (LEAVE A REPLY)

NEW QUESTION: 73
An IT administrator needs to quickly identify all devices connected to a specific subnet within their network.
They decide to use the search feature to find all IP addresses within the 10.0.0.0/8 subnet.
Which search term should they use?
A. 10.0.0.0/16
B. 10.
C. 10.0.0
Answer: B (LEAVE A REPLY)
The search bar in the ClearPass Endpoints and Access Tracker views supports partial-string matching. To find all devices in the 10.x.x.x (10/8) range, simply typing "10." will filter the list to show every entry where the IP address field begins with those two characters. This is the most efficient way to perform broad subnet filtering without using complex query syntax.

NEW QUESTION: 74
Which of the following is NOT a typical role of ClearPass in a network?
A. Device authentication
B. Network intrusion detection
C. Policy enforcement
D. Guest access management
Answer: (SHOW ANSWER)

While ClearPass plays a crucial role in authentication, policy enforcement, and guest access management, it does not directly function as a network intrusion detection system (IDS).

NEW QUESTION: 75
An organization wants to enforce role-based access policies across their entire network to ensure that users have appropriate access privileges regardless of their connection point. How does ClearPass facilitate this requirement?
A. By providing detailed audit logs of all network activity
B. By offering customizable user authentication methods
C. By allowing the creation of individual user roles with associated privileges that applies anywhere on the network
Answer: C (LEAVE A REPLY)
ClearPass enables role-based access control (RBAC) by allowing administrators to create individual user roles with defined privileges that are enforced consistently across wired, wireless, and VPN connections. This ensures that users maintain the same level of network access regardless of where or how they connect.

NEW QUESTION: 76
A healthcare organization uses ClearPass to secure its network. All employees use personal laptops, which must be provisioned via Onboard and evaluated for antivirus and OS patch status before accessing internal systems. If a device is non-compliant, it should be redirected to a remediation VLAN.
Which three ClearPass configurations are required to support this requirement? (Choose three)
Response:
A. Onboard provisioning portal with certificate issuance
B. Active Directory domain join script in the Guest module
C. MAC address bypass rules for personal laptops
D. Enforcement policy to redirect non-compliant devices
E. OnGuard posture policy with antivirus and patch checks
Answer: (SHOW ANSWER)

NEW QUESTION: 77
If a guest user must sponsor themselves using their own email address, what is a critical step to ensure they can access the network?
A. Complete a phone verification process.
B. Submit a secondary form for verification.
C. Verify their email address before access is granted.
Answer: (SHOW ANSWER)
Self-sponsorship is a security risk because any user can create an account. To mitigate this, ClearPass should require Email Verification . After registering, the user's account remains in a restricted state until they click a unique link sent to their provided email address. This confirms the user has access to a legitimate email account and provides an audit trail for the organization.

NEW QUESTION: 78
An organization uses ClearPass to verify client certificates for network access. A client attempts to authenticate using a TLS certificate. What does ClearPass need to verify to ensure the certificate is valid?
A. ClearPass only needs to verify the issuing date and timestamp.
B. ClearPass must verify the certificate's issuing organization and the client's private key.
C. ClearPass must verify the certificate's issuing organization, issuing date, and timestamp within the allowed clock skew.
Answer: C (LEAVE A REPLY)
To validate a client TLS certificate, ClearPass verifies that the certificate is issued by a trusted organization and that it is currently valid based on its issuance and expiration timestamps. Time validation is performed within an allowed clock skew to account for minor time differences between systems.

NEW QUESTION: 79
An IT administrator is setting up ClearPass servers for a new network environment. They need to ensure that the RADIUS authentication will work seamlessly across all servers in the cluster.
What crucial step must they take regarding the certificates?
A. Share a single RadSec certificate across all servers
B. Install a single certificate on the publisher server only
C. Install certificates individually on every ClearPass server
Answer: C (LEAVE A REPLY)
Each ClearPass server in a cluster terminates RADIUS and TLS connections independently. To ensure consistent and seamless RADIUS authentication across the

cluster, valid certificates must be installed on every ClearPass server so that all nodes can securely handle authentication requests.

NEW QUESTION: 80
Which two elements are typically configured inside a ClearPass Enforcement Policy? (Choose two)
Response:
A. ClearPass system logging
B. DNS server IP allocation
C. RADIUS Access-Accept reply attributes
D. VLAN ID assignment
Answer: (SHOW ANSWER)

NEW QUESTION: 81
An IT administrator needs to ensure that requests to different Active Directory servers in a multinational company are properly filtered. How should they configure the network?
A. Create multiple Network Device Groups and filter requests by "belongs to group."
B. Rely on the default settings of the Active Directory servers for request filtering.
C. Use a single Network Device Group for all sites and filter requests by IP address.
Answer: A (LEAVE A REPLY)
Comprehensive and Detailed Explanation From HPE Aruba Networking ClearPass portfolio:
Network Device Groups (NDGs) allow administrators to categorize switches and controllers by location or function. In a multi-site deployment, ClearPass can use a "Service Rule" that looks at which NDG the request came from. For example, if a request comes from the "London-Switches" group, ClearPass is configured to use the London AD domain; if it comes from "Tokyo-APs," it uses the Tokyo AD source. This prevents "cross-talk" between global regions and improves authentication speed.

NEW QUESTION: 82
What does ClearPass OnGuard use to determine an endpoint's compliance posture?
Response:
A. NAT table inspections
B. Persistent or dissolvable health agents
C. Active Directory OU mapping
D. Syslog parsing
Answer: (SHOW ANSWER)

NEW QUESTION: 83

An organization uses ClearPass to manage network access for its devices. A device reported as stolen is detected attempting to connect to the network. What action can the EMM server trigger upon receiving an HTTP API call from ClearPass?
A. The EMM server can automatically block all network traffic from the device.
B. The EMM server can send a message to the user or wipe the user's device.
C. The EMM server can permanently disable the device's network interface.
Answer: B (LEAVE A REPLY)
ClearPass and EMM/MDM integration provides "Closed-Loop" security. When ClearPass identifies a
"Stolen" device status (either via its own database or a real-time check), it can use a Context Server Action to signal the EMM server. The EMM server, which has deep administrative control over the device OS, can then execute high-level security commands such as Remote Wipe (deleting all data) or displaying a "Lock Screen" message to the person holding the device.

NEW QUESTION: 84
An IT administrator is configuring ClearPass to send guest receipts for registrations. They want to ensure that guests receive these receipts through both email and SMS simultaneously. What steps should the administrator follow to achieve this configuration?
A. Configure both the email relay and SMS gateway in the Messaging Setup menu.
B. Navigate to Administration > External Servers > Guest Setup to configure messaging.
C. Use the REST API to manually send emails and SMS messages.
Answer: A (LEAVE A REPLY)
To send guest receipts via both email and SMS, the administrator must configure the email relay and SMS gateway in the Messaging Setup menu. This enables ClearPass Guest to deliver registration notifications through multiple communication channels simultaneously.

NEW QUESTION: 85
A company has implemented ClearPass Policy Manager to manage network access. ClearPass gathers user credentials, endpoint profile context, and the client's health status during a network access request. Which stage of the ClearPass process is responsible for making this final decision and replying to the request?
A. Profile Information Gathering
B. Roles and Enforcement process
C. Service Selection
Answer: (SHOW ANSWER)
After the initial authentication and context-gathering stages, ClearPass enters the Roles and Enforcement phase. During Role Mapping, ClearPass assigns one or more internal roles based on the gathered data. The Enforcement Policy then evaluates these roles against defined rules to make the final "Allow" or "Deny" decision. This stage is responsible

for selecting the Enforcement Profile, which contains the final RADIUS attributes (like VLANs or ACLs) sent back to the Network Access Device.

NEW QUESTION: 86
An IT administrator needs to monitor the network for authentication failures of high-priority devices and receive notifications in near-real-time. Which feature of the ClearPass Insight reporting tool should they use to accomplish this task?
A. Audit trails
B. Customized reports
C. Alerts
Answer: C (LEAVE A REPLY)
ClearPass Insight alerts are designed to provide near-real-time notifications based on defined conditions, such as authentication failures for high-priority devices. This allows administrators to proactively monitor critical events and respond quickly.

NEW QUESTION: 87
A company wants to provide downloadable PDF guides for guests accessing their network. The IT team has uploaded the PDFs to the Content Manager. How should they configure these files to ensure guests can access them via the web server?
A. Store the PDFs in the private files section of the Content Manager.
B. Apply a skin that includes links to the PDFs.
C. Store the PDFs in the public files section of the Content Manager.
Answer: C (LEAVE A REPLY)
The ClearPass Content Manager distinguishes between "Private" and "Public" storage. Public files are accessible to any user who can reach the ClearPass web server, even if they have not yet authenticated. This is essential for guest onboarding guides or maps, as the user needs to download these files before they have the credentials to fully join the network.

NEW QUESTION: 88
An IT administrator is configuring a Web-Based Health Check service in ClearPass to enforce posture compliance for client endpoints. They need to ensure that the service can handle requests from various operating systems and networks. Which step should the administrator take to ensure the posture policy is applied correctly to the agent's System Health Validator report?
A. Select the Posture Compliance option to add the Posture tab to the service.
B. Configure the service without specifying the operating system for the agent.
C. Assign multiple Posture Policies to the same client endpoint.
Answer: (SHOW ANSWER)
Selecting the Posture Compliance option enables the Posture tab within the service configuration.

This allows ClearPass to evaluate the System Health Validator report generated by the web- based agent and correctly apply the defined posture policy across different operating systems and network environments.

NEW QUESTION: 89
An IT administrator wants to improve the user experience during the login process by reducing unnecessary redirects and ensuring users receive immediate feedback on credential validity. Which approach should the administrator implement?
A. Configure the NAD to handle more simultaneous connections.
B. Increase the timeout period for RADIUS communication.
C. Enable the pre-authentication check in the ClearPass login process.
Answer: C (LEAVE A REPLY)
Without Pre-Authentication , a user might submit incorrect credentials, be redirected to the controller, have the controller send a RADIUS request, and then be redirected back to the portal with an error message. This
"ping-pong" effect is slow and confusing. Enabling the pre-authentication check allows ClearPass to validate the credentials immediately while the user is still on the web page, providing instant feedback and eliminating the extra redirects for failed attempts.

NEW QUESTION: 90
A company has deployed ClearPass Onboard to manage their BYOD environment. They want to ensure that each device connecting to the network has a unique identity for auditing purposes.
Additionally, they are considering integrating ClearPass with Aruba Central Client Insights to enhance profiling accuracy using AI and ML. Which feature of ClearPass Onboard directly supports the company's need for unique device identities?
A. ClearPass Onboard supports anti-virus and firewall checks for device compliance.
B. ClearPass Onboard provides endpoint compliance and control capabilities.
C. ClearPass Onboard assigns a unique certificate to each device that goes through the Onboard process.
Answer: C (LEAVE A REPLY)
ClearPass Onboard issues a unique device certificate to each endpoint during the onboarding process. This certificate-based identity uniquely identifies every device on the network, enabling precise auditing, strong authentication, and long-term device tracking independent of user credentials.

NEW QUESTION: 91
An IT specialist is tasked with ensuring that guests receive their login credentials via SMS after completing the self-registration process. What configuration must be checked to guarantee that this feature is enabled?
A. The network must disable email notifications to enable SMS notifications.

B. ClearPass must be configured to send the guest account information via SMS.
C. The guest's browser must support SMS messaging.
Answer: B (LEAVE A REPLY)
ClearPass Guest must be configured with an SMS delivery option so that guest account credentials are sent via SMS after self-registration. This requires proper SMS gateway integration and enabling SMS as a credential delivery method within the guest workflow.

NEW QUESTION: 92
A network administrator is configuring a corporate network enforcement policy. The policy includes rules for corporate-issued laptops, MDM-enabled tablets, and personal smart devices.
However, the administrator notices that some clients are failing all rules due to a lack of profile data. What should the administrator do to ensure these unprofiled clients can access the profiler collectors and receive a profile using best practices?
A. Add a rule that identifies clients without profiles and assigns them a role allowing limited access to the profiler.
B. Increase the frequency of profile data updates from the endpoint profiler.
C. Set the default enforcement profile to 'Allow Access' for all unprofiled clients.
Answer: (SHOW ANSWER)
The best practice is to add a rule that detects unprofiled clients and assigns them a limited-access role that permits communication with the profiler collectors. This approach allows ClearPass to gather profiling data securely while preventing unverified devices from gaining unrestricted network access.

NEW QUESTION: 93
Which two actions can ClearPass take based on posture evaluation results?
(Choose two)
Response:
A. Redirect non-compliant devices to remediation VLAN
B. Assign guest portal login page
C. Enforce quarantine access with limited permissions
D. Issue digital certificates to unknown devices

Answer: A,C (LEAVE A REPLY)

NEW QUESTION: 94
An IT administrator attempts to join a ClearPass server to an Active Directory domain. They notice that the system clocks of the ClearPass server and the AD domain are not in sync. The ClearPass server is 10 minutes behind the AD domain. What will be the likely outcome of this attempt to join the domain?
A. The join will succeed but ClearPass will generate a warning about the clock skew.
B. The join will succeed because ClearPass automatically adjusts the clock skew during the join process.
C. The join will fail because Active Directory only allows a maximum of five minutes of clock skew.
Answer: C (LEAVE A REPLY)
Kerberos, the underlying protocol for Active Directory authentication, is extremely time-sensitive. To prevent
"replay attacks," AD Domain Controllers strictly enforce a maximum clock skew of 5 minutes . If the ClearPass server's clock differs from the AD domain by 10 minutes, the Kerberos tickets will be considered invalid, and the domain join attempt will fail . Administrators must ensure both systems are synced to a reliable NTP source before joining.

NEW QUESTION: 95
A security analyst needs to ensure that ClearPass sends a notification whenever a report is ready. They want to receive these notifications via SMS. What is the correct procedure to set this up?
A. Set up an email relay and configure it to forward the emails as SMS messages.
B. Configure the SMS Gateway under ClearPass Guest and ensure report notifications are enabled in Insight.
C. Enable SMS notifications in the Administration > External Servers > Messaging Setup menu.
Answer: (SHOW ANSWER)
To send SMS notifications, ClearPass must have a configured SMS Gateway (typically found under the Guest module's configuration). Once the gateway is functional, the ClearPass Insight reporting engine can be configured to trigger a notification to a specific phone number or administrator group whenever a scheduled report is generated or a system alert is triggered.

NEW QUESTION: 96
An IT administrator is managing a network with ClearPass and notices that one of the devices is sending multiple health checks throughout the day via different networks (wired, wireless, and VPN). How does OnGuard handle the license usage for this device?

A. OnGuard debits one license per day for the device regardless of the number of health checks or networks used.
B. OnGuard debits a license for each network the device connects to throughout the day.
C. OnGuard debits a separate license for each health check sent by the device.
Answer: A (LEAVE A REPLY)
ClearPass OnGuard licensing is based on the unique endpoint, not the number of connections or checks. A single device that connects via wired in the morning, Wi-Fi in the afternoon, and VPN in the evening- triggering a health check each time-will only consume one OnGuard license for that 24-hour period. This
"per-device" model makes licensing predictable for enterprise deployments with roaming users.

NEW QUESTION: 97
Which protocol is commonly used by ClearPass to communicate with network devices for enforcing access control decisions?
Response:
A. HTTP
B. NTP
C. RADIUS
D. SNMP
Answer: C (LEAVE A REPLY)

NEW QUESTION: 98
An IT specialist is configuring authentication methods for a network resource in ClearPass. They need to ensure that only valid methods are used and that the client credentials are authenticated against multiple sources in a specific order. What should the specialist do?
A. Use the Authorization tab to configure authentication methods
B. Add new RADIUS COA Action for each authentication source
C. Select multiple authentication sources and order them from top-down
Answer: (SHOW ANSWER)
ClearPass services are designed to be flexible with identity sources. In the Authentication tab of a service configuration, an administrator can add multiple sources (e.g., Active Directory, Guest Repository, and Local User Repository). ClearPass processes these sources in the exact order they appear in the list-attempting to authenticate the user against the first source, and moving to the next only if the user is not found in the previous one.

NEW QUESTION: 99
Which two conditions can be used in ClearPass Service Rules to match incoming authentication requests?
(Choose two)

Response:
A. Antivirus status
B. MAC address vendor
C. RADIUS NAS-Port-Type
D. Time of day
Answer: C,D (LEAVE A REPLY)

NEW QUESTION: 100
Which two tasks can be scheduled in ClearPass for system maintenance?
(Choose two)
Response:
A. Configuration replication to switches
B. Backup exports to external storage
C. Enforcement policy simulation
D. Automatic log cleanup
Answer: B,D (LEAVE A REPLY)

NEW QUESTION: 101
A network administrator needs to revoke a certificate for a lost device to ensure it no longer has network access. They navigate to the Certificate Authorities section in ClearPass Onboard. What next step should they take to ensure the certificate is properly revoked and the device is blocked?
A. Select the certificate authority, edit the retention policy to store only metadata, and then revoke the certificate.
B. Select the certificate authority, view the issued certificates, and revoke the specific certificate associated with the lost device.
C. Select the certificate authority, view the trust chain, and manually revoke the certificate from the list.
Answer: (SHOW ANSWER)
To manage certificates in ClearPass Onboard, the administrator must drill down into the specific Certificate Authority (CA) that issued the credentials. From there, they can view a list of all issued certificates , search for the one belonging to the lost device (using the username or MAC address), and perform the Revoke action. This immediately invalidates the certificate for future 802.1X authentications.

NEW QUESTION: 102
A company needs to add a new field to an existing form and wants it to appear before a specific field already on the form. What is the correct sequence of actions to meet this need?
A. Select the existing field in the forms editor and choose the 'Insert Before' option.

B. Use the Customize Form Field workspace to drag and drop the new field before the existing one.
C. Select the existing field in the forms editor and choose the 'Insert After' option.
Answer: (SHOW ANSWER)
ClearPass Guest's Form Editor provides contextual placement for new fields. To ensure a field appears in a specific order, the administrator should first highlight the field that will follow the new one. By selecting
'Insert Before' , the editor places the new field directly above the selected item in the form's logical flow, ensuring the user sees the questions in the intended sequence.

NEW QUESTION: 103
A company is setting up a custom Enforcement Profile for operator logins in ClearPass. They decide to copy an existing operator login profile and modify the value of the admin_privileges attribute. What additional step must they take to properly assign this custom profile to the users?
A. Create a new role in the Admin User Repository and link it to the custom profile.
B. Create an application enforcement policy and modify the rules to include the new custom profile.
C. Assign the custom profile directly to users in the Local User Repository.
Answer: A (LEAVE A REPLY)
Operator logins (logins to the CPPM/Guest/Onboard admin interfaces) are managed by the Admin User Repository . To apply a custom enforcement profile, you must first define a new Role that signifies those specific privileges. You then create a rule in the admin enforcement policy that says: "If User has [New Role], then apply [Custom Enforcement Profile] ." This links the user's identity to the specific administrative rights you've defined.

NEW QUESTION: 104
An IT administrator notices that endpoints are being re-evaluated with the same enforcement decisions even after client status changes. They realize this is causing inefficient network access control. What could be the underlying issue?
A. The client devices are not compliant with the network security policies.
B. The service is configured to reset posture and role status every time.
C. The 'Use Cached Results' option is not enabled on the enforcement tab.
Answer: C (LEAVE A REPLY)
If cached results are not enabled on the Enforcement tab, ClearPass repeatedly reprocesses policy evaluations instead of reusing previously computed posture and role decisions. This causes the same enforcement outcomes to be applied even after client status changes, leading to inefficient access control behavior.

NEW QUESTION: 105

An IT administrator is setting up a captive portal for a company's network and needs to ensure that the SSL certificate is compatible with the Aruba Instant device they are using. Which type of certificate should the administrator install to meet this requirement?
A. CER certificate
B. PEM certificate
C. DER certificate
Answer: (SHOW ANSWER)
Network access devices, including Aruba Instant APs and controllers, generally require certificates in the PEM (Privacy Enhanced Mail) format. PEM certificates are Base64 encoded and are standard for Unix- based systems and networking hardware because they can easily include the entire trust chain (server, intermediate, and root certificates) in a single text file.

NEW QUESTION: 106
An IT specialist is tasked with setting up ClearPass to ensure requests are processed by the appropriate service. They notice that different network access types require different service processing methods. How should the specialist configure ClearPass?
A. Create a universal service that handles all types of requests.
B. Filter the services list to focus on the stack of services for the specific type of request.
C. Configure all services using the Wizards and Service Templates.
Answer: B (LEAVE A REPLY)
ClearPass installations often contain dozens of services. To keep the policy logic manageable, administrators use Service Groups or Filtering . By categorizing services based on access type (e.g., all "802.1X Wireless" services together), the specialist can focus on the specific "stack" of rules that apply to a request. This organization makes it easier to verify that more specific rules are prioritized correctly over generic ones.

NEW QUESTION: 107
Where in ClearPass is the user role finally linked to an enforcement action such as VLAN assignment?
Response:
A. Enforcement Policy

B. Monitoring Dashboard
C. Policy Simulation Tool
D. Endpoint Context Server
Answer: A (LEAVE A REPLY)

NEW QUESTION: 108
Which ClearPass feature allows organizations to enforce limited access for unauthenticated guests?
Response:
A. Captive Portal
B. Pre-Auth Check
C. Enforcement Policy
D. MAC Caching
Answer: A (LEAVE A REPLY)

NEW QUESTION: 109
What is the purpose of configuring a self-registration page in ClearPass Guest?
Response:
A. To allow internal users to reset passwords
B. To enable guest users to create accounts without IT intervention
C. To provide IP addresses to guest users
D. To manage 802.1X certificates for BYOD devices
Answer: B (LEAVE A REPLY)

NEW QUESTION: 110
An organization needs to configure a secure 802.1X wired service in ClearPass to manage access on their network. They want to ensure that different device types have different security profiles. Which feature of ClearPass should they use to achieve this?
A. Enforcement profiles with profiling
B. Port security with MAC address tracking
C. MAC Authentication without profiling
Answer: (SHOW ANSWER)
To differentiate security levels based on device type (e.g., giving a VoIP phone different access than a laptop), ClearPass must use Profiling . The service first identifies the device type using various collectors and then evaluates this information in the Enforcement Policy . This allows the administrator to select specific Enforcement Profiles (VLANs/ACLs) that are dynamically assigned based on the high-fidelity profile data gathered at connection time.

NEW QUESTION: 111

A network admin wants to configure a ClearPass service that dynamically applies a VLAN based on the user's Active Directory group membership. Which three configurations are required in ClearPass to implement this behavior?
(Choose three)
Response:
A. Static MAC authentication bypass list
B. Enforcement Policy with VLAN profiles
C. Role Mapping Policy based on AD groups
D. Authentication Source with AD integration
E. Web-based authentication method
Answer: B,C,D (LEAVE A REPLY)

NEW QUESTION: 112
A network administrator is configuring a new Network Access Device (NAD) in ClearPass. They select RadSec for the network device and notice that the PSK field automatically changes to 'radsec' regardless of what is typed. What is the most likely reason for this behavior?
A. RadSec requires a fixed PSK value for secure communication.
B. The network device is not compatible with RadSec configuration.
C. The administrator's user permissions restrict changes to the PSK field.
Answer: A (LEAVE A REPLY)
As discussed in Q5, RadSec utilizes TLS for security, which renders the traditional RADIUS MD5 shared secret obsolete. In the ClearPass interface, when RadSec is selected as the protocol, the system automatically defaults the PSK to 'radsec' because the underlying communication is now secured by certificates, not a password. This is a standard behavior of the protocol implementation in HPE Aruba products to indicate that certificate-based trust is now the priority.

NEW QUESTION: 113
An IT specialist is tasked with setting up ClearPass to ensure requests are processed by the appropriate service. They notice that different network access types require different service processing methods. How should the specialist configure ClearPass to handle this requirement?
A. Create a universal service that handles all types of requests.
B. Filter the services list to focus on the stack of services for the specific type of request.
C. Configure all services using the Wizards and Service Templates.
Answer: (SHOW ANSWER)
ClearPass processes requests by evaluating services in a logical stack based on request type.
Filtering the services list to the relevant service type ensures that only appropriate services are evaluated, allowing requests to be matched and processed correctly and efficiently.

NEW QUESTION: 114
A client connects to a network and initially has the attribute 'IsProfiled=false'. The client is placed in a
'Limited Access to the Profiler' role. What sequence of events will occur next to ensure the client gains full access to the network?
A. ClearPass immediately profiles the client upon connection, and the client is granted full access without any further steps.
B. The client sends a DHCP request, ClearPass profiles the client, sends a terminate session instruction, and the client re-authenticates with full access.
C. The client sends a DHCP request, ClearPass profiles the client and grants full access without terminating the session.
Answer: (SHOW ANSWER)
This is the "Profile and Bounce" workflow.
* Initial connection: Device is unknown (IsProfiled=false) and restricted.
* The device sends a DHCP request , which is intercepted by the ClearPass Profiler.
* ClearPass identifies the device (e.g., "Company Laptop") and updates the database.
* To apply the new "Full Access" policy, ClearPass must trigger a RADIUS CoA Terminate-Session to the NAD.
* The device immediately reconnects and authenticates again; this time, ClearPass sees the updated profile and grants full access.

NEW QUESTION: 115
A client connects to a network and initially has the attribute 'IsProfiled=false'. The client is placed in a 'Limited Access to the Profiler' role. What sequence of events will occur next to ensure the client gains full access to the network?
A. ClearPass immediately profiles the client upon connection, and the client is granted full access without any further steps.
B. The client sends a DHCP request, ClearPass profiles the client, sends a terminate session instruction, and the client re-authenticates with full access.
C. The client sends a DHCP request, ClearPass profiles the client and grants full access without terminating the session.
Answer: B (LEAVE A REPLY)
When a client with 'IsProfiled=false' connects, it is initially given limited access to allow profiling traffic (such as DHCP). ClearPass profiles the device based on this traffic, then sends a terminate session command to trigger re-authentication. Once re-authenticated with updated profiling information, the client is assigned a full-access role.

NEW QUESTION: 116
What two ClearPass features work together to deliver dynamic segmentation based on user context?

(Choose two)
Response:
A. Log Archiving
B. Device Profiling
C. Guest Self-Registration
D. Role Mapping
Answer: (SHOW ANSWER)

NEW QUESTION: 117
Which two actions can be configured within a ClearPass Guest self-registration workflow? (Choose two)
Response:
A. Enforcing MAC-based VLAN assignment
B. Sending SMS with login credentials
C. Requiring sponsor approval
D. Encrypting RADIUS traffic
Answer: B,C (LEAVE A REPLY)

NEW QUESTION: 118
In a network using ClearPass with 802.1X authentication and a dissolvable agent, a client is granted limited access with a captive portal redirect. After the client runs the health check via the webpage, what critical step must be taken to ensure the updated posture token is used in subsequent authentications?
A. ClearPass must send a termination message to the client to enforce a new role.
B. The client must restart their device to apply the updated posture token.
C. The posture token must be cached in the service by selecting the Cached Policies and Roles option on the 802.1X service Enforcement tab.
Answer: (SHOW ANSWER)
Because the health check is performed via a web interface (WEBAUTH), it is a separate transaction from the original 802.1X request. For the 802.1X service to "see" the result of that health check during the next authentication, the token must be stored. Enabling "Cached Policies and Roles" allows ClearPass to hold the posture status in memory and apply it to the user's primary connection once they re-authenticate.

NEW QUESTION: 119
A network administrator is troubleshooting an issue where endpoints are not receiving updated enforcement decisions after a second authentication. What is the most likely configuration change needed?
A. Disable the "Use Cached Results" on enforcement tab.
B. Disable endpoint re-authentication.
C. Increase the frequency of the posture checks.

Answer: (SHOW ANSWER)
If "Use Cached Results" is enabled in the enforcement configuration, ClearPass may continue to apply the same access level from the previous authentication attempt without re-evaluating the current data. Disabling this feature forces ClearPass to perform a fresh evaluation of the endpoint's attributes-including any newly updated posture tokens from OnGuard-every time a re-authentication occurs.

NEW QUESTION: 120
What is the primary function of Aruba ClearPass?
A. Manage network switches
B. Authenticate network devices and users
C. Monitor network performance
D. Optimize network throughput
Answer: B (LEAVE A REPLY)
Aruba ClearPass is primarily used for network access control, allowing organizations to authenticate, authorize, and enforce policies for users and devices connecting to the network.

NEW QUESTION: 121
In a corporate network following Zero Trust best practices, a security team notices unusual activity from a previously authenticated and authorized device. What should the team do next to ensure the network's security?
A. Increase the device's access privileges to monitor more closely.
B. Ignore the activity since the device was already authenticated.
C. Reduce the device's privileges or quarantine it for further investigation.
Answer: (SHOW ANSWER)
Zero Trust security assumes that trust is never permanent. When unusual behavior is detected, access must be dynamically adjusted by reducing privileges or quarantining the device to prevent potential threats while the activity is investigated.

NEW QUESTION: 122

Which two administrative actions help ensure database integrity and secure access in ClearPass?
(Choose two)
Response:
A. Configuring role-based access for admin logins
B. Disabling TACACS+ for internal users
C. Enabling NTP synchronization across nodes
D. Encrypting database backups
Answer: (SHOW ANSWER)

NEW QUESTION: 123
Which ClearPass feature can be used to profile endpoints and determine device types?
Response:
A. Insight
B. Guest Self-Registration
C. Device Profiling
D. Access Tracker
Answer: C (LEAVE A REPLY)

NEW QUESTION: 124
An IT administrator is configuring ClearPass to connect to an AD server. They decide to set the server timeout to 20 seconds. What potential issue might arise from this configuration?
A. The AD server will reject the connection from ClearPass.
B. The backup AD server will be contacted immediately, bypassing the primary server.
C. The client may timeout before ClearPass has time to contact a second AD server.
Answer: C (LEAVE A REPLY)
Client devices (supplicants) have their own internal RADIUS timers, often defaulting to 5-10 seconds. If ClearPass is configured with a long 20-second timeout for its primary AD source, and that server is unresponsive, ClearPass will wait the full 20 seconds before failing over to a backup source. By that time, the client device has likely already timed out and given up on the connection, resulting in an authentication failure for the user. Standard practice is to keep AD timeouts short (e.g., 3-5 seconds).