HP

HPE6-A88

HPE Networking ClearPass

Questions & Answers (Demo)

Version: 4.0

Question: 1

In a university setting where users often connect more than five devices to the network, an IT administrator notices some devices are problematic and require frequent upgrades. How can ClearPass assist in identifying the impact of these upgrades?

A. By profiling devices and allowing the administrator to see the types and number of devices affected quickly

B. By blocking all problematic devices from connecting to the network

C. By automatically upgrading all devices to the latest firmware

Answer: A

Explanation:

ClearPass Profiling is a foundational feature used to gain visibility into every device on the network. It uses various "collectors" (such as DHCP fingerprints, HTTP User-Agents, and MAC OUIs) to determine the Category, OS Family, and Name of an endpoint. In a high-density environment like a

university, profiling allows administrators to generate reports on specific device types. When an upgrade is required for a specific model (e.g., a specific version of Android or a certain laptop brand), the administrator can instantly see exactly how many of those devices are currently active, allowing for better capacity planning and impact analysis.

Question: 2

A company has recently shifted to a zero-trust model and is facing challenges with its legacy network infrastructure, which was not designed for such a model. The company is particularly concerned about the security of its network as it accommodates a growing number of remote users and IoT devices. What solution could help them create role-based access policies and ensure continuous, closed-loop security across their network?

A. Implementing ClearPass to enable role-based access policies and device profiling.

B. Adding more traditional firewalls to strengthen the network perimeter.

C. Deploying additional VPNs for remote user access.

Answer: A

Explanation:

The Zero Trust framework dictates that "trust" is never granted implicitly but is instead based on identity and context. ClearPass provides this by moving security away from static IP/VLAN-based rules to Dynamic Role-Based Access Control (RBAC). By integrating profiling (to identify what the device is) with authentication (to identify who the user is), ClearPass assigns a "Role." This role stays with the user/device regardless of where or how they connect, ensuring a consistent security posture across legacy and modern infrastructure.

Question: 3

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

Explanation:

ClearPass is designed as an open platform. The External Context Server feature allows ClearPass to exchange data with third-party security systems like Firewalls (Palo Alto, Check Point), EMM/MDM (Intune, AirWatch), and SIEMs (Splunk). By using REST APIs or XML/JSON over HTTP, ClearPass can send "Context Server Actions" (like telling a firewall to quarantine a user) or receive data to be used as attributes in authorization policies.

Question: 4

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

Explanation:

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.

Question: 5

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

Explanation:

RadSec (RADIUS over TLS) replaces the traditional MD5-based Pre-Shared Key (PSK) with a secure TLS tunnel. While the UI might show a placeholder "radsec" PSK, the actual security relies on Mutual Authentication via certificates. For the TLS handshake to succeed, ClearPass must trust the Certificate

Authority (CA) that signed the NAD's certificate, and vice versa. Therefore, verifying that the NAD's trust chain is uploaded to the ClearPass Trust List is the most critical step for a successful connection.