DUMPSARENA

Selling HPE Aruba Networking Solutions

HP HPE2-W12

Version Demo

Total Demo Questions: 6

Total Premium Questions: 63

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

A senior IT manager tells you that she wants IT staff members to spend less time troubleshooting issues so they have more time to focus on new initiatives. How can HPE Aruba Networking deliver the senior IT managerâ€™s desired outcome?

A. HPE Aruba Networking ClearPass monitors network devicesâ€™ performance and automatically notifies IT admins of performance issues.

B. HPE Aruba User Experience Insight (UXI) helps IT determine why data center applications are not performing as well as they should.

C. HPE Aruba Networking Edge-to-Cloud solutions rely on AI to automate the onboarding of devices.

D. HPE Aruba Networking Central with AI for Networking accelerates troubleshooting by providing insights and recommendations that help remedy issues.

ANSWER: D

Explanation:

HPE Aruba Networking Central with AI for Networking accelerates troubleshooting by providing insights and recommendations that help remedy issues. Aruba Central applies AIOps capabilities to network telemetry, identifying anomalous behavior and correlating information across the network to help operations teams isolate the likely cause of a problem more quickly. Its AI Insights surface conditions that merit attention, while AI Assist and guided recommendations provide useful operational context for resolving incidents. This changes troubleshooting from a largely manual, reactive activity into a more proactive, data-driven workflow.

For the senior IT manager's objective, the key outcome is reduced operational effort and faster resolution of network issues. By shortening investigation and remediation cycles, Central helps reduce mean time to resolution and allows IT staff to devote less time to routine troubleshooting. The resulting capacity can be redirected toward strategic projects, modernization, and other new initiatives. Aruba describes Central as a cloud-based networking management platform with AI-powered operations designed to simplify network operations and improve operational efficiency. See the Aruba Central product page and the Aruba AIOps overview.

QUESTION NO: 2

A healthcare organization has thousands of connected clinical and facilities devices, many of which cannot run endpoint agents. Security staff need to identify unknown devices, distinguish device types, and use that information to make more appropriate access-policy decisions. Which HPE Aruba Networking capability should you emphasize?

A. HPE Aruba Networking Fabric Composer

B. HPE Aruba Networking Central Client Insights

C. HPE Aruba Networking EdgeConnect SD-WAN

D. HPE Aruba Networking User Experience Insight (UXI)

ANSWER: B

Explanation:

HPE Aruba Networking Central Client Insights provides AI-based discovery and profiling of devices connected to the network. It helps organizations identify managed, unmanaged, BYOD, and IoT endpoints and establish greater confidence in device identity before applying access policies.

ClearPass Policy Manager can enforce access decisions, but the decisive requirement is first to discover and classify a broad population of devices, including headless IoT devices. Fabric Composer and EdgeConnect SD-WAN do not provide this endpoint-profiling function.

QUESTION NO: 3

A managed service provider must deploy standardized network configurations to hundreds of customer locations. The provider wants devices to receive their intended configuration when they first connect, without requiring an engineer to configure each device on site. Which HPE Aruba Networking Central capability should you emphasize?

A. AI-based security recommendations for firmware upgrades

B. Client Insights device profiling

C. Zero-touch provisioning with centralized configuration

D. Dynamic Segmentation role assignment

ANSWER: C

Explanation:

Zero-touch provisioning is the relevant HPE Aruba Networking Central capability. It allows devices to be onboarded and provisioned from centralized templates and configuration workflows, reducing the need for local technical resources during deployment.

AI Insights helps identify operational issues after telemetry is collected, and Client Insights profiles connected endpoints. Dynamic Segmentation applies access policy, but it does not replace the initial device deployment and configuration workflow required by the provider.

QUESTION NO: 4

A customer expresses this key business objective of wanting to deploy IoT more securely. What is one way HPE Aruba Networking solutions help customers achieve this goal?

A. HPE Aruba Networking solutions identify various types of IoT devices with high confidence and offer policy recommendations to make it simple to implement least privilege access.

B. HPE Aruba Networking Fabric Composer helps customers build secure tunnels between IoT devices and the data center, where the IoT traffic is segmented and filtered to eliminate threats.

C. HPE Aruba Networking is the only vendor to offer endpoint security agents specifically designed for IoT devices.

D. HPE Aruba Networking is the first vendor to achieve ICSA Labs' certification for IoT inventory management.

ANSWER: A

Explanation:

HPE Aruba Networking solutions identify various types of IoT devices with high confidence and offer policy recommendations to make it simple to implement least privilege access. This directly supports secure IoT deployment because organizations must first know what is connecting to the network before they can apply appropriate controls. Aruba Central Client Insights uses AI-based device profiling to identify and classify connected clients, including unmanaged and headless IoT devices. ClearPass Device Insight extends this visibility with continuous device discovery and classification, helping security teams understand device attributes and behavior without relying on endpoint agents. After a device is identified, the organization can use that context to assign suitable access privileges and enforce policy through Aruba's security architecture. Applying least-privilege access limits an IoT device to only the network resources, applications, and services required for its intended function. This reduces exposure from devices that may be difficult to patch, manage, or secure directly. The combination of accurate device intelligence, recommended policy actions, and context-based access enforcement enables customers to scale IoT adoption while maintaining stronger control and reducing operational complexity. Aruba describes these capabilities in its Client Insights overview and ClearPass Device Insight overview.

QUESTION NO: 5

A customer wants to know what makes HPE Aruba Networking ZTNA better than a traditional virtual private network (VPN). What is one key distinguishing value?

A. The cloud-based solution seamlessly scales to accommodate customers' growing remote workforce.

B. HPE Aruba Networking ZTNA decreases complexity with its on-prem management platform.

C. HPE Aruba Networking ZTNA shrinks the attack surface by automatically creating and applying least-privilege policies.

D. The cost of the solution is lower than a traditional VPN because HPE Aruba Networking ZTNA uses HPE Aruba Networking gateways.

ANSWER: C

Explanation:

HPE Aruba Networking ZTNA shrinks the attack surface by automatically creating and applying least-privilege policies. This is a central Zero Trust distinction: access is granted to a specific private application or resource after evaluating the user identity, device posture, and other contextual signals, rather than placing the user broadly onto the private network. The connection is therefore application-level and policy-driven, which limits the resources exposed to each user and helps contain risk if an account or endpoint is compromised.

Aruba's Security Service Edge platform delivers ZTNA as part of a cloud-delivered security architecture. Its policies can continuously enforce access decisions and provide secure connectivity to private applications without exposing those applications directly to the internet. By applying least privilege automatically and dynamically, the solution supports secure remote and third-party access while reducing opportunities for unnecessary access and lateral movement. This is the key customer value when contrasting ZTNA with traditional remote-access approaches. HPE Aruba Networking describes its SSE and ZTNA capabilities at HPE Aruba Networking Secure Access Service Edge and provides further Zero Trust guidance at HPE's Zero Trust Security overview.

QUESTION NO: 6

Which business outcome is a high priority for most Chief Information Security Officers (CISO)?

A. Allowing network admins to use their preferred security monitoring tools.

B. Ensuring that employees can only access resources from within the corporate campus.

C. Improving operational continuity by minimizing risks and attack surfaces.

D. Planning network security so that they can assume no breach will ever occur.

ANSWER: C

Explanation:

Improving operational continuity by minimizing risks and attack surfaces is a core business outcome for a CISO because security leadership is accountable for helping the organization remain resilient, trustworthy, and able to operate through evolving cyber threats. Reducing the attack surface limits the number of exposed systems, identities, devices, and pathways that adversaries can target. Reducing risk through consistent controls, visibility, segmentation, and access policies lowers the likelihood that a security incident will disrupt essential services. These measures support continuity by enabling the business to prevent incidents where possible and contain their impact when they occur. This outcome also aligns with a modern zero-trust approach: organizations continuously verify access, apply least privilege, and protect users, devices, applications, and data wherever work takes place. Aruba describes zero trust as an approach that reduces organizational risk through continuous verification and least-privilege access, while its security portfolio emphasizes reducing exposure and strengthening protection across distributed environments. These capabilities help security teams protect business operations rather than merely administer isolated security tools. See Aruba's Zero Trust Security for Dummies resource and HPE Aruba Networking Security.