PassQueen
a.k.a dumpsqueen.com

Aruba Certified Clearpass Professional v6.2

Aruba ACCP-v6.2

Version Demo

Total Demo Questions: 16

Total Premium Questions: 160

Buy Premium PDF

https://passqueen.com

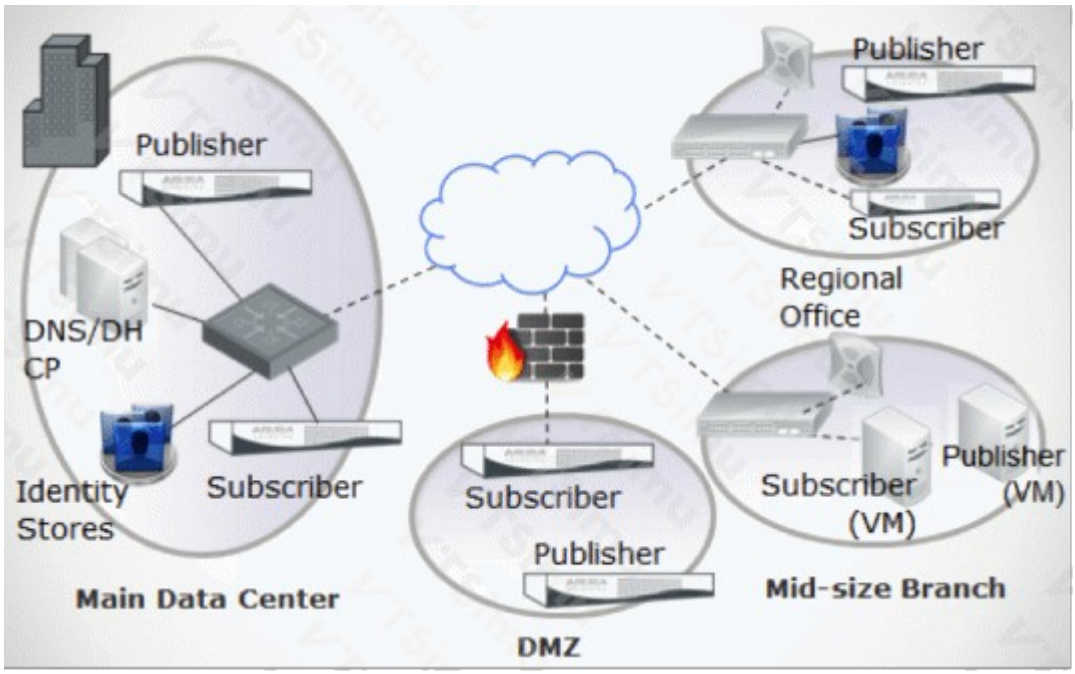
support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, ClearPass Policy Manager	88
Topic 2, ClearPass Guest	30
Topic 3, ClearPass Onboard	23
Topic 4, ClearPass OnGuard	12
Topic 5, ClearPass Insight	5
Topic 6, Mix Questions	2
Total	160

QUESTION NO: 1

Below is a network topology diagram:



How many clusters are needed for this deployment?

A. 1

B. 3

C. 4

D. 8

E. 2

ANSWER: C

Explanation:

4 is correct because the topology represents four distinct ClearPass deployment locations, each requiring its own local ClearPass cluster. A ClearPass cluster is a group of Policy Manager servers that share configuration and provide redundancy and load distribution within a deployment site. The servers assigned to one cluster must have reliable, low-latency connectivity so that database replication, configuration synchronization, and cluster communication remain dependable. For a geographically distributed design, independent local clusters allow authentication and policy decisions to continue at each location without depending on a WAN connection to another site. Each cluster can also provide high availability for its local access devices and endpoints while maintaining an appropriate separation between the sites shown in the topology. Aruba's ClearPass documentation describes clustering as the mechanism for operating multiple Policy Manager servers together for redundancy and scale, and its deployment guidance emphasizes designing clusters around suitable network connectivity and latency requirements. See the Aruba ClearPass Cluster Overview and ClearPass clustering documentation.

QUESTION NO: 2

A Publisher node in a cluster goes down and Subscribers are no longer able to reach the publisher. Which of the following is true? (Choose 2).

A. Users authenticating with the Publisher node continue to authenticate.

B. Users authenticating with the Subscriber nodes are no longer able to authenticate.

C. Users authenticating with the Publisher node are no longer able to authenticate.

D. Users authenticating with the Subscriber nodes continue to authenticate.

E. No users can authenticate to either the Publisher or Subscriber nodes.

ANSWER: C D

Explanation:

Users authenticating with the Publisher node are no longer able to authenticate because the Publisher is the cluster member that has failed and therefore cannot receive, process, or respond to RADIUS/TACACS+ authentication requests. Availability of services directed specifically to that appliance is lost until the node is restored or network access to it is re-established.

Users authenticating with the Subscriber nodes continue to authenticate because ClearPass Policy Manager Subscriber appliances are active policy-service nodes. They maintain the information required to evaluate requests and make enforcement decisions locally, including the replicated configuration and policy data received from the Publisher. Authentication processing does not require a real-time connection to the Publisher for every client request. Consequently, a loss of Publisher reachability prevents configuration synchronization and centralized administrative changes from being propagated during the outage, but it does not inherently stop the Subscriber Policy Manager services from processing authentications. This cluster design allows network access services to remain available when the Publisher is unavailable, provided that network devices are configured to send requests to reachable Subscriber nodes and those nodes' dependent services remain available. Aruba's clustering guidance describes the Publisher as the configuration master and Subscribers as nodes that replicate configuration while providing policy services. See the Aruba ClearPass cluster deployment documentation and the ClearPass cluster overview.

QUESTION NO: 3

Which of the following components of a Policy Service is mandatory?

A. Enforcement

B. Posture

C. Profiler

D. Role Mapping Policy

E. Authorization Source

ANSWER: A

Explanation:

Enforcement is mandatory because a ClearPass Policy Service must have an enforcement policy selected to produce the authorization decision returned after a request is processed. The enforcement policy evaluates the conditions associated with the authenticated connection and selects an enforcement profile or other resulting action. Those profiles define what ClearPass sends to the network access device, such as an assigned role, VLAN, downloadable user role, access-control list, or a deny response. In practical terms, enforcement is the part of the service that converts ClearPass policy evaluation into an actionable RADIUS response for the requesting device.

ClearPass Policy Manager organizes service processing around rules and policy components, with the enforcement configuration supplying the final access decision for the service. This makes Enforcement the required component among the listed choices. Aruba's Policy Manager documentation describes services and their enforcement-policy processing in the ClearPass Policy Manager Services documentation. Additional Aruba guidance on creating and applying enforcement policies is available in the Enforcement Policies documentation.

QUESTION NO: 4

Refer to the screen capture below:

Based on the Enforcement Policy configuration, if a user with Role Engineer connects to the network and the posture token assigned is Unknown, what Enforcement Profile will be applied?

A. EMPLOYEE_VLAN

B. Remote Employee ACL

C. RestrictedACL

D. Deny Access Profile

E. HR VLAN

ANSWER: D

Explanation:

Deny Access Profile will be applied. ClearPass evaluates enforcement-policy rules in their configured order and applies the enforcement profile associated with the first rule whose conditions match the authenticated session. For the stated session, the user has the *Engineer* role, but the posture token is *Unknown*. An Unknown posture result means ClearPass does not have a posture state that qualifies the endpoint for normal network access under a posture-dependent authorization rule. The policy configuration therefore directs this role-and-posture combination to the deny enforcement action. Applying a deny profile is an appropriate access-control outcome when endpoint health cannot be established, because it prevents the session from receiving production access until posture can be successfully evaluated and an acceptable token is returned. Aruba ClearPass enforcement policies use role, posture, and other session attributes to select an enforcement profile, and the profile delivers the resulting authorization action to the network device. Aruba's ClearPass documentation describes enforcement policies and profiles in the Enforcement Policies documentation and provides additional policy-management guidance in the Policy Manager User Guide.

QUESTION NO: 5

An administrator wants to assign a different Aruba user role to employees and contractors after successful 802.1X authentication. The employee and contractor identities are stored in Active Directory groups.

Which ClearPass component should be used to map the Active Directory group membership to local ClearPass roles?

A. Role Mapping Policy

B. Enforcement Profile

C. Posture Policy

D. Service Rule

E. Authentication Method

ANSWER: A

Explanation:

Role Mapping Policy is correct. A ClearPass Role Mapping Policy evaluates attributes returned from authorization sources, including Active Directory group membership, and assigns local ClearPass roles when its rules match. The resulting roles are then available to the Enforcement Policy, which selects the Aruba user role or other enforcement result returned to the network access device.

An Enforcement Policy uses roles and other session attributes to select enforcement profiles, but it does not perform the initial mapping of directory attributes into local ClearPass roles. Aruba documents role mapping as the policy stage used to map authorization attributes to ClearPass roles in the ClearPass Role Mapping documentation.

QUESTION NO: 6

What is the Onboard license usage based on?

A. Each user connected to the provisioning SSID uses 1 Onboard license.

B. Each user authenticated using the Onboard credential uses 1 Onboard license.

C. Each user provisioned using the Onboard process uses 1 Onboard license.

D. Each user that has the OnGuard agent downloaded uses 1 Onboard license.

E. Each user that downloads the Onboard application to their iOS device uses 1 Onboard license.

ANSWER: C

Explanation:

Each user provisioned using the Onboard process uses 1 Onboard license. ClearPass Onboard is the certificate-based device provisioning component of ClearPass Policy Manager. During the Onboard workflow, ClearPass creates and issues a device credential—typically a certificate—and installs the required profile or configuration on the user's device. License consumption is therefore associated with completing this provisioning process for a user, rather than with merely joining a provisioning network, downloading an application, installing an OnGuard agent, or later authenticating with a credential that has already been provisioned.

In practical terms, Onboard licensing measures the population of users enabled for certificate-based onboarding. A user who has completed Onboard provisioning consumes an Onboard license, and ClearPass tracks that usage through its licensing framework. This model aligns capacity with the number of users for whom ClearPass performs the identity and credential-provisioning service. Aruba's ClearPass documentation describes Onboard as the solution for provisioning devices with certificates and configuration profiles, while ClearPass licensing documentation explains that licensed application capacity is managed from Policy Manager's licensing functions. See the ClearPass Onboard documentation and the ClearPass license management documentation.

QUESTION NO: 7

Below is a screenshot of the Guest Role Mapping Policy:

What is the purpose of this Role Mapping Policy?

A. To send a firewall role back to the controller based on the Guest User's Role ID.

B. To assign Controller roles to guests.

C. To display a role name on the Self-registration receipt page.

D. To assign ClearPass roles to guests based on the guest's Role ID as seen during authentication.

E. To assign all 3 roles of [Contractor], [Guest] and [Employee] to every guest user.

ANSWER: D

Explanation:

To assign ClearPass roles to guests based on the guest's Role ID as seen during authentication is correct because a ClearPass Role Mapping Policy evaluates authorization attributes gathered during authentication and translates matching attribute values into internal ClearPass roles. In a Guest workflow, the Role ID associated with the guest account is available as an attribute when the user authenticates. Rules in the Guest Role Mapping Policy can test that Role ID and, when a rule matches, assign the corresponding ClearPass role, such as a guest, contractor, or employee-related role.

The resulting ClearPass role is an internal policy value used later in service enforcement decisions. It allows enforcement logic to consistently apply the access treatment associated with the authenticated guest's assigned Guest role, without relying solely on the raw Role ID value. This is the intended purpose of role mapping: normalize attributes from an authentication or identity source into roles that Policy Manager can use in subsequent authorization and enforcement processing. Aruba's Policy Manager documentation describes role-mapping policies as the mechanism for mapping authorization-source attributes to ClearPass roles, and its Guest documentation explains the role-based attributes available for guest accounts. See Aruba ClearPass Role Mapping Policies and Aruba ClearPass Guest Accounts.

QUESTION NO: 8

Which of the following statements are true about a ClearPass Publisher in a cluster? (Choose 2)

A. The Publisher is the configuration master for the cluster.

B. Subscribers receive replicated configuration from the Publisher.

C. All configuration changes must be made independently on every Subscriber.

D. A Subscriber cannot process RADIUS authentication requests.

E. The Publisher is used only for Guest web login pages.

ANSWER: A B

Explanation:

The Publisher is the configuration master for the cluster. is true. Administrative configuration changes are made on the Publisher, which maintains the authoritative cluster configuration and replicates that configuration to Subscriber nodes.

Subscribers receive replicated configuration from the Publisher. is also true. Subscribers use the replicated configuration to process authentication and authorization requests locally. This architecture enables Subscribers to provide policy services while centralizing configuration management on the Publisher. Aruba describes Publisher and Subscriber responsibilities in the ClearPass Cluster Overview.

QUESTION NO: 9

Which of the following is true about Data and Management ports on the ClearPass appliance? (Choose 2)

A. Configuration of the data port is optional.

B. Configuration of the data port is mandatory.

C. Configuration of the management port is optional.

D. Configuration of the management port is mandatory.

E. Static IP addresses are only allowed on the management port.

ANSWER: A D

Explanation:

ClearPass appliances separate administration-oriented connectivity from service/data-plane connectivity. Configuration of the management port is mandatory because ClearPass requires a reachable management interface for initial appliance setup and for ongoing administrative access to Policy Manager, including browser-based administration, CLI access, and cluster-management communication. During deployment, an IP address, netmask, and gateway are assigned to this interface so that the appliance can be managed on the network.

Configuration of the data port is optional. The data interface is intended for ClearPass service traffic, such as RADIUS authentication and accounting exchanges, and it can be configured when an organization wants to separate that traffic from management traffic or implement a particular network design. A single configured management interface is sufficient for a supported basic deployment, while a data interface is added when required by the deployment architecture. Aruba's installation documentation describes management-interface network configuration as part of appliance initialization and identifies the data interface as an optional additional interface. See the Aruba ClearPass hardware appliance installation documentation and the ClearPass initial setup documentation.

QUESTION NO: 10

Which of the following are valid reasons for ClearPass to reject an EAP-TLS client certificate? (Choose 2)

A. The client certificate has expired.

B. The issuing CA is not trusted by ClearPass.

C. The user did not enter a password.

D. The NAD does not have a client certificate.

E. The client did not configure a pre-shared key.

ANSWER: A B

Explanation:

The certificate has expired and **the issuing CA is not trusted by ClearPass** are valid reasons for an EAP-TLS authentication failure. During certificate-based authentication, ClearPass validates the client certificate against the configured trust chain and checks certificate validity information. A certificate that is outside its valid date range or that cannot be chained to a trusted CA does not satisfy the EAP-TLS authentication requirements.

EAP-TLS does not use a username and password as the client credential. The client proves its identity by presenting a valid certificate and demonstrating possession of the corresponding private key. See RFC 5216: EAP-TLS and the ClearPass 6.2 documentation.

QUESTION NO: 11

A Hospital would like to deploy ClearPass Guest for friends and relatives of patients to access the Internet. They would like patients to be able to access an internal webpage on the intranet where they can view patient information. However, other guests should not have access to this page.

Which of the following is true? (Choose 2)

A. The NAD device will be firewalling users to block Intranet traffic.

B. ClearPass will be firewalling users to block Intranet traffic.

C. It's necessary for us to have two separate web login pages due to the different access requirements of patients and guests.

D. We will need to configure different Enforcement actions for patients and guests in the service.

E. Both the NAD and Clearpass would have to firewall users to block traffic.

ANSWER: A D

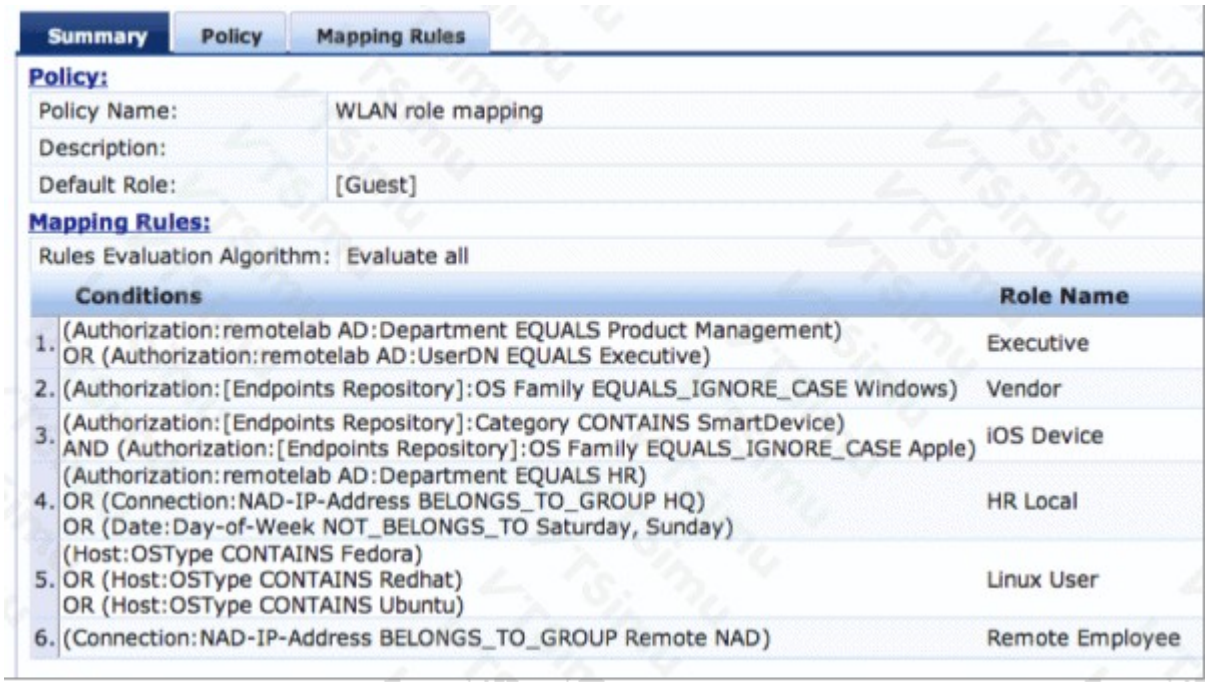
Explanation:

The NAD device will be firewalling users to block Intranet traffic. ClearPass Policy Manager is the policy decision point: it authenticates the user, evaluates role-mapping and enforcement policy rules, and returns enforcement attributes to the network access device (NAD). The NAD, such as an Aruba controller, gateway, switch, or compatible wireless device, is the policy enforcement point. It applies the returned role, VLAN assignment, downloadable user role, or ACL/firewall policy to control the traffic that the authenticated client can send. Consequently, an Internet-only guest policy can prevent access to private intranet destinations, while a patient policy can permit the required internal web resource.

We will need to configure different Enforcement actions for patients and guests in the service. The ClearPass service needs policy outcomes appropriate to each identity category. Role-mapping rules can classify successful logins as patients or ordinary guests based on the selected authentication source, account attributes, guest role, or other session context. Enforcement rules can then return distinct NAD-consumable access controls: for example, a patient role that permits the authorized intranet web application in addition to Internet access, and a guest role that provides Internet-only access. This centralizes identity-aware policy decisions in ClearPass while ensuring that actual packet filtering occurs on the NAD. Aruba's Policy Manager documentation describes enforcement policies and profiles as the mechanism for returning these access-control decisions to network devices: Aruba ClearPass Enforcement Policies and Aruba ClearPass Enforcement Profiles.

QUESTION NO: 12

Refer to the screen capture below



Summary | Policy | Mapping Rules

Policy:

Policy Name:	WLAN role mapping
Description:	
Default Role:	[Guest]

Mapping Rules:

Rules Evaluation Algorithm: Evaluate all

	Conditions	Role Name
1.	(Authorization:remotelab AD:Department EQUALS Product Management) OR (Authorization:remotelab AD:UserDN EQUALS Executive)	Executive
2.	(Authorization:[Endpoints Repository]:OS Family EQUALS_IGNORE_CASE Windows)	Vendor
3.	(Authorization:[Endpoints Repository]:Category CONTAINS SmartDevice) AND (Authorization:[Endpoints Repository]:OS Family EQUALS_IGNORE_CASE Apple)	iOS Device
4.	(Authorization:remotelab AD:Department EQUALS HR) OR (Connection:NAD-IP-Address BELONGS_TO_GROUP HQ) OR (Date:Day-of-Week NOT_BELONGS_TO Saturday, Sunday)	HR Local
5.	(Host:OSType CONTAINS Fedora) OR (Host:OSType CONTAINS Redhat) OR (Host:OSType CONTAINS Ubuntu)	Linux User
6.	(Connection:NAD-IP-Address BELONGS_TO_GROUP Remote NAD)	Remote Employee

If a user from the department "HR" connects on Monday to a switch that belongs to the Device Group Remote NAD, what roles are assigned to the user in Clearpass? (Choose 2)

A. Executive

B. Remote Employee

C. iOS Device

D. Guest

E. HR Local

ANSWER: B E

Explanation:

The roles assigned are **Remote Employee** and **HR Local**. ClearPass evaluates the role-mapping rules against the session attributes received during authentication and can assign more than one role when more than one rule matches. The connection through a switch in the *Remote NAD* device group satisfies the rule that assigns the **Remote Employee** role. Separately, the user's HR department attribute, together with the Monday condition shown in the role-mapping configuration, satisfies the rule that assigns **HR Local**. The role name itself is simply a label configured by the administrator; ClearPass assigns it when that rule's conditions evaluate as true, regardless of whether the label might appear counterintuitive in relation to the NAD group name. These roles are accumulated in the request context and can then be used by the enforcement policy to select the appropriate enforcement profile, such as a VLAN, downloadable user role, or access-control decision. Aruba documents that role-mapping policies derive one or more roles from authentication and authorization attributes, and that those roles are subsequently available to enforcement decisions. See the ClearPass Policy Manager role-mapping policy documentation and the ClearPass enforcement policy documentation.

QUESTION NO: 13

Which of the following is true? (Choose 2)

A. Mobile Device Management is used to control device usage post-onboarding

B. Mobile Device Management is an application container that is used to provision work applications

C. Mobile Device Management cannot be deployed without Workspace

D. 3rd party Mobile Device Management solutions can be integrated with Clearpass

E. Mobile Device Management cannot do remote wipes of devices without workspace being installed

ANSWER: A D

Explanation:

Mobile Device Management is used to control device usage post-onboarding because MDM platforms apply and maintain management policies after a device has been enrolled. Those controls can include configuration profiles, compliance requirements, restrictions, application deployment, inventory collection, and security actions. In a ClearPass deployment, this post-enrollment management state is valuable because it supplies device attributes—such as whether a device is enrolled, compliant, or otherwise managed—that can be used in access-control decisions. ClearPass can therefore distinguish managed devices from unmanaged devices and apply the organization's network-access policy appropriately.

3rd party Mobile Device Management solutions can be integrated with Clearpass because ClearPass Policy Manager includes MDM integration capabilities for gathering device-management and compliance information from supported external MDM services. ClearPass can query or receive relevant endpoint context and use that context in its policy evaluation and enforcement workflow. This allows an organization to retain its chosen MDM product while using ClearPass for identity-aware network access control across wired, wireless, and VPN environments. Aruba's ClearPass documentation describes MDM integration as part of endpoint-context and policy capabilities; see the ClearPass MDM integration overview and the ClearPass Policy Manager documentation.

QUESTION NO: 14

Refer to the screenshot below:

Based on the above configuration which of the following statements is true?

A. Only guest users connecting to SSID Aruba will be allowed access to the network by ClearPass Guest.

B. The minimum password length for guest passwords is set to a default value of 8.

C. The usernames generated for guest users by Guest Manager will be a combination of random numbers.

D. The password generated for guest users by Guest Manager will be a combination of random numbers.

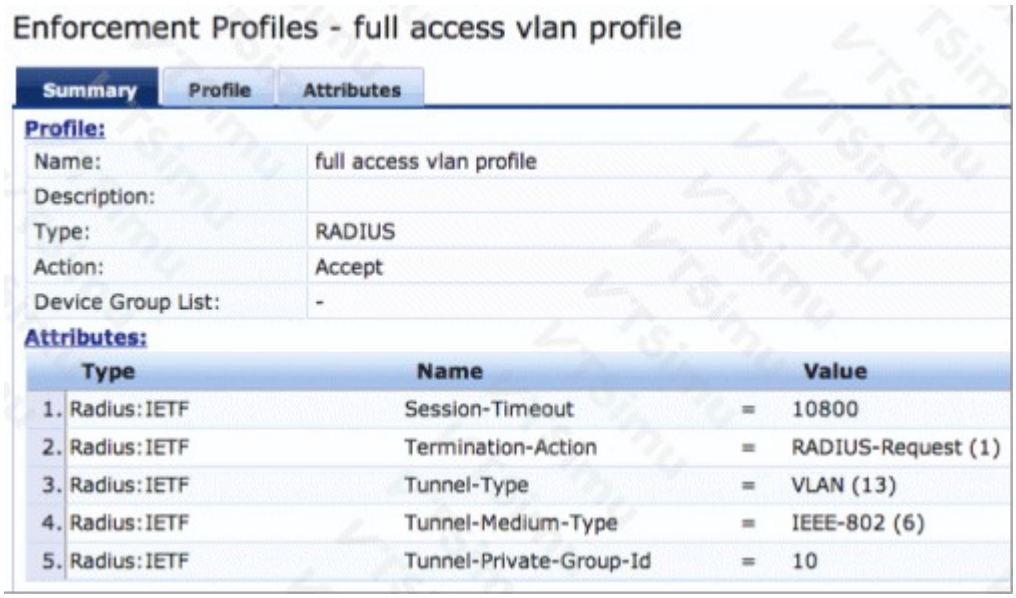
ANSWER: D

Explanation:

The password generated for guest users by Guest Manager will be a combination of random numbers. The configuration shown sets the guest-password generation format to numeric random values. When an operator creates a guest account through ClearPass Guest Manager, ClearPass applies the configured password-generation rule to the account rather than requiring the operator to manually define a password. This is useful for short-lived visitor credentials because the generated password can be printed, displayed on a receipt, or sent to the guest while retaining the configured format and length policy. Guest Manager derives account credentials from the active guest-account configuration and its random-generation settings; therefore, a numeric password format results in passwords composed of randomly generated digits. This behavior concerns the credentials issued during guest-account creation and does not by itself define a particular wireless SSID or an access-control decision. Aruba's ClearPass Guest documentation describes guest-account creation and the configurable username and password generation settings used by Guest Manager. See the Aruba ClearPass Guest User Accounts reference and the Aruba ClearPass Guest Manager reference.

QUESTION NO: 15

Refer to the following configuration for a VLAN Enforcement Policy:



Enforcement Profiles - full access vlan profile

Summary | Profile | Attributes

Profile:

Name:	full access vlan profile
Description:	
Type:	RADIUS
Action:	Accept
Device Group List:	-

Attributes:

	Type	Name		Value
1.	Radius:IETF	Session-Timeout	=	10800
2.	Radius:IETF	Termination-Action	=	RADIUS-Request (1)
3.	Radius:IETF	Tunnel-Type	=	VLAN (13)
4.	Radius:IETF	Tunnel-Medium-Type	=	IEEE-802 (6)
5.	Radius:IETF	Tunnel-Private-Group-Id	=	10

Based on the profile configuration, which of the following VLANs will be assigned to the user when this profile is used?

A. VLAN 13

B. VLAN 6

C. VLAN 10

D. VLAN 1

E. VLAN 10800

ANSWER: C

Explanation:

VLAN 10 will be assigned because the VLAN Enforcement profile is configured with a VLAN ID of 10. When ClearPass returns this enforcement profile as the result of policy evaluation, it supplies the VLAN assignment in the RADIUS authorization response. The network access device—such as an Aruba switch or controller—uses that returned VLAN identifier to place the authenticated user's session into the corresponding VLAN. The effective assignment is therefore based on the profile's configured VLAN ID, rather than on unrelated values that may appear elsewhere in the configuration or device context.

In ClearPass, VLAN enforcement is an authorization action: authentication establishes the user identity, policy determines the applicable enforcement result, and the enforcement profile communicates the VLAN assignment to the access device.

For a successful dynamic VLAN assignment, the access device must also be configured to accept RADIUS-assigned VLAN attributes and have VLAN 10 available. Aruba's ClearPass documentation describes enforcement profiles and their use in returning authorization actions to network devices; Aruba's wired-access documentation further describes RADIUS-based role and VLAN assignment. See the ClearPass Policy Manager Enforcement Profiles documentation and the Aruba AOS-CX RADIUS VLAN assignment documentation.

QUESTION NO: 16

A customer would like to deploy ClearPass with the following objectives: Every day, 100 employees authenticate with their corporate laptops using EAP-TLS. Every Friday, there is a meeting with business partners and an additional 50 devices authenticate using Web Login Guest Authentication.

Which of the following is correct? (Choose 2)

A. When counting policy manager licenses, they need to include the additional 50 business partner devices

B. When counting policy manager licenses, they can exclude the additional 50 business partner devices

C. They should purchase guest licenses

D. They should purchase onboard licenses

E. They should purchase onguard licenses

ANSWER: B C

Explanation:

They can exclude the additional 50 business partner devices when calculating Policy Manager licenses because those devices use the ClearPass Guest web-login workflow rather than the Policy Manager access-license pool used for employee device authentication. The 100 corporate laptops authenticating through EAP-TLS are managed endpoints and establish the Policy Manager capacity requirement. ClearPass licensing distinguishes access control for managed endpoints from Guest functionality, allowing guest users to be licensed through the dedicated Guest license model.

They should purchase guest licenses because the partner devices require Web Login Guest Authentication. Guest licenses provide the ClearPass Guest entitlement and capacity needed to create, manage, and authenticate guest accounts and devices. Since the meeting occurs weekly, the relevant Guest capacity should accommodate the maximum simultaneous guest demand: 50 partner devices during the Friday meeting. The organization should therefore size Policy Manager licensing for its corporate EAP-TLS endpoints and separately ensure that its Guest licensing covers the expected guest population.

Aruba's ClearPass documentation describes licensing and the distinct license types available for Policy Manager and Guest services in the ClearPass License Management guide. Additional ClearPass product and licensing resources are available from Aruba ClearPass.