PassQueen
a.k.a dumpsqueen.com

Pulse Connect Secure (PCS): Administration and Configuration

Pulse Secure PCS

Version Demo

Total Demo Questions: 12

Total Premium Questions: 121

Buy Premium PDF

https://passqueen.com

support@passqueen.com

QUESTION NO: 1

Which Single Sign-On (SSO) policy relies on the Connect Secure domain name?

A. Headers/Cookies

B. Basic Auth/NTLM

C. Form POST

D. SAML

ANSWER: D

Explanation:

SAML is correct because Pulse Connect Secure uses its configured domain name as part of the SAML identity-provider context presented to a service provider. In a SAML SSO deployment, Connect Secure issues SAML assertions for authenticated users and exposes identity-provider endpoints and metadata whose URLs are based on the appliance's externally reachable, configured domain name. The service provider must recognize that identity-provider identity and use the corresponding endpoint URLs when initiating authentication or receiving a SAML response.

Accordingly, the Connect Secure domain name needs to be accurate, resolvable by users and the service provider where applicable, and consistent with the URL and certificate configuration used for the SAML exchange. This ensures that SAML requests, assertion-consumer responses, issuer identifiers, and metadata references point to the intended Connect Secure identity provider. Pulse Secure's administration documentation specifically identifies SAML SSO as the SSO policy that relies on the Connect Secure domain name. See the official Pulse Connect Secure Administration Guide: About Single Sign-On and the Pulse Secure Technical Publications portal.

QUESTION NO: 2

When configuring a realm to require multiple sign-in credentials, which three are valid secondary authentication methods? (Choose three.)

A. Active Directory

B. Client certificate

C. RADIUS

D. LDAP

E. Netegrity

ANSWER: A C D

Explanation:

Pulse Connect Secure realms can be configured for layered authentication, requiring users to satisfy a primary authentication process and an additional authentication server before access is granted. Active Directory is a supported secondary method because PCS can use an AD authentication server to validate a user's directory credentials as part of the realm's authentication policy. RADIUS is also supported for secondary authentication, enabling an organization to add a centrally managed RADIUS-backed credential challenge, including common MFA or token-based deployments exposed through RADIUS. LDAP is valid for the same purpose: PCS can query an LDAP authentication server as an additional credential-validation step for users in the realm.

Using these server types lets administrators combine an initial identity check with a second sign-in credential requirement while preserving centralized user and group management. The authentication servers must be configured under the PCS authentication-server configuration and then selected in the realm's authentication policy. Ivanti's Pulse Connect Secure

product documentation and support resources describe the supported authentication-server integrations and realm authentication configuration: Pulse Connect Secure Administration Guide and Ivanti Product Documentation.

QUESTION NO: 3

Core web access provides support for which applications? (Choose three.)

A. Java applications

B. Web applications

C. Point to Point applications

D. HTML5 VDI

ANSWER: A B C

Explanation:

Core web access supports **Java applications**, **Web applications**, and **Point to Point applications**. This access model is delivered through the PCS web portal and is designed to make internal resources available without requiring a full network-layer VPN connection for every use case. Web applications are accessed through the PCS reverse-proxy and content-rewriting capabilities, allowing authorized users to reach internal HTTP/HTTPS resources through the portal. Java applications are supported through the platform's Java application-access capabilities. Point to Point applications are supported for approved client/server application flows, allowing PCS to proxy or tunnel the specific application connection rather than exposing unrestricted network access. Administrators configure these resources and their associated access-control policies so that users receive only the application access granted by their roles. This application-oriented approach is a core PCS security benefit because it can limit access to defined resources rather than broadly extending internal network reachability. Pulse Secure's administrator documentation describes Web access and Core Access as the application-access framework for web, Java, and client/server/point-to-point resources. See the Pulse Connect Secure Core Access documentation and the Pulse Connect Secure Web Access documentation.

QUESTION NO: 4

What Access Management Framework function determines what internal system users can access?

A. Authentication Realm

B. User Role

C. Resource Policy

D. Resource Profile

ANSWER: B

Explanation:

User Role is correct because roles define the access entitlement assigned to an authenticated user in the Pulse Secure Access Management Framework. After a user's identity is validated through an authentication realm, Pulse Connect Secure evaluates role-mapping rules and assigns one or more user roles. Those roles determine the user's effective access experience and authorize access to internal resources and services through the policies associated with the role. In practical terms, a role represents the organization's authorization decision: for example, a contractor, employee, administrator, or partner can be placed into distinct roles with different permitted internal applications, networks, bookmarks, or resource policies. This separation allows administrators to authenticate users centrally while applying access rights according to business function, group membership, device posture, or other mapped attributes. Resource-access settings are therefore delivered in the context of the user role, making User Role the framework function that determines what internal systems and resources a user may access. Pulse Secure's documentation describes access control as an authentication, role-mapping, and role-based authorization workflow. See the Pulse Secure Device Access Management Framework guide and the Ivanti Connect Secure Administration Guide.

QUESTION NO: 5

For how many days will a PCS continue to work if the license server is not working (grace period)?

A. 10

B. 20

C. 30

D. 40

ANSWER: A

Explanation:

10 is correct. Pulse Connect Secure uses a license-server connectivity grace period to avoid an immediate service interruption when the appliance cannot contact its configured licensing server. During this period, the PCS appliance continues operating with its existing licensed capacity, allowing administrators time to restore license-server reachability without abruptly disrupting remote-access users. The documented grace period is 10 days. The period is specifically relevant when the licensing service is unavailable or unreachable; it is not a replacement for maintaining a valid license or for restoring the licensing infrastructure. Administrators should therefore investigate DNS, routing, firewall policy, certificate, and licensing-server service health as soon as the appliance reports a licensing communication issue. Once connectivity is restored, PCS can resume normal license validation. Pulse Secure's licensing guidance identifies the 10-day interval among the important operational facts for appliances that cannot reach the license server. See the official Pulse Secure knowledge-base article, KB22374, for the documented licensing-server grace-period behavior. For current product documentation and support resources, consult the Ivanti Connect Secure documentation portal.

QUESTION NO: 6

Which two statements about certificate-based user authentication are true? (Choose two.)

A. Certificate-based user authentication may not require user input during the authentication exchange.

B. Certificate attributes can be used to determine the correct sign-in page.

C. Certificate attributes can be used to assign users to roles.

D. Certificate-based user authentication requires the use of OCSP.

ANSWER: A C

Explanation:

Certificate-based user authentication may not require user input during the authentication exchange. With client-certificate authentication, the user's browser or device presents an installed X.509 client certificate during the TLS handshake. If the certificate is available and accepted by the configured authentication realm, PCS can identify and authenticate the user without prompting for a separate username and password. The user might still need to select a certificate when multiple certificates are available, but additional credential entry is not inherently required.

Certificate attributes can be used to assign users to roles. PCS can inspect certificate subject and issuer information, including distinguished-name components and other certificate fields, when evaluating role-mapping rules. This lets an administrator map authenticated users to the appropriate access roles based on identity data embedded in their client certificates. Role assignment is therefore integrated with certificate authentication and can support differentiated access policies without relying exclusively on directory group lookup. For configuration concepts and authentication/role-mapping guidance, see the Ivanti Connect Secure documentation and the Ivanti product documentation portal.

QUESTION NO: 7

Pulse Policy Secure supports multiple authentication servers including: (Choose three.)

A. Active Directory

B. Local servers

C. LDAP

D. RADIUS

E. XForce

ANSWER: A B C D

Explanation:

Pulse Policy Secure supports Active Directory, Local servers, LDAP, and RADIUS as authentication-server types. Active Directory integration enables PPS to authenticate users against Microsoft AD domains and use directory attributes for policy decisions. Local servers provide an internal user database on the PPS appliance, which is useful for local administrative, test, guest, or contingency accounts. LDAP support enables authentication against standards-based LDAP directory services. RADIUS support lets PPS delegate authentication to a RADIUS server, including environments that use RADIUS as the access point for MFA, tokens, or other centralized authentication services. Therefore, the question is incorrectly constrained to “Choose three,” because four of the supplied technologies are valid PPS authentication-server options. XForce is not an authentication-server type; it is associated with security intelligence and threat-information services rather than a user identity store or authentication protocol. The PPS Administration Guide lists the supported authentication-server configuration categories, including Active Directory, LDAP, RADIUS, and local authentication. See the Pulse Policy Secure Administration Guide: Authentication Servers and the IETF RADIUS specification for the protocol’s role in centralized network access authentication.

QUESTION NO: 8

Which element cannot be configured when creating Web Resource Profiles?

A. Specify web access control policy.

B. Specify a realm to assign the profile.

C. Specify authentication policies.

D. Specify a Base URL.

E. Assign roles to the bookmark.

ANSWER: A

Explanation:

Specify web access control policy. is correct because a Web Resource Profile defines the web application resource and its profile-specific settings, such as the application’s base URL and the access context used for the published resource. Web access control is not configured as an element of the profile-creation workflow itself. Instead, access decisions for web traffic are governed through the applicable access-control and resource-policy configuration, which is evaluated when users request protected content. This separation lets an administrator define a reusable web resource profile for an application while managing authorization behavior through the policy framework rather than embedding a web access-control policy directly in the profile. Pulse Secure’s Web Resource Profile documentation identifies the profile settings and describes how the profile is associated with user access and web-resource behavior; it does not make a web access-control policy a configurable profile attribute. See the Pulse Secure Defining a Web Resource Profile documentation and the Ivanti Connect Secure Administration Guide for the current policy and resource-configuration model.

QUESTION NO: 9

You have configured your PCS device to use OCSP for certificate validation. Which statement is true?

A. The PCS device will validate certificates with the OCSP server on an on-demand basis.

B. The PCS device will download the CRL from the OCSP server.

C. The PCS device will periodically check user certificates with the OCSP server.

D. The PCS device will use OCSP to download and validate the CA certificate.

ANSWER: A

Explanation:

The PCS device will validate certificates with the OCSP server on an on-demand basis. OCSP is a certificate-status validation mechanism in which PCS sends a status request to the configured responder when it needs to determine whether a certificate is valid or has been revoked. The responder returns a signed status response for the specific certificate, allowing PCS to make the validation decision without relying on a locally downloaded and periodically refreshed certificate revocation list.

In PCS trusted-server certificate validation settings, enabling OCSP causes PCS to use the configured OCSP responder for these certificate-status checks. This behavior is appropriately described as on-demand: the appliance checks certificate status as part of the validation workflow rather than treating OCSP as a scheduled certificate-checking process. This use of OCSP aligns with the protocol definition, which provides current status information for an identified certificate through a responder request and response. For PCS configuration details, see the PCS Administration Guide: Configuring Options for Trusted Server Certificates. The OCSP protocol is specified in RFC 6960.

QUESTION NO: 10

Which methods of access can be used to support clientless access to internal systems using the Telnet protocol? (Choose two.)

A. Telnet.exe

B. Core Java

C. Core HTML5

D. Pulse SAM

ANSWER: B C

Explanation:

Core Java and **Core HTML5** are the browser-delivered methods that Pulse Connect Secure supports for clientless Telnet access. With Core Java, PCS provides a Java-based terminal emulation experience through the user's browser, allowing the user to establish a Telnet session to an internal resource without installing or configuring a full VPN client. This approach was intended for environments where the Java browser capability was available and permitted by policy.

Core HTML5 provides the corresponding browser-native approach. PCS uses HTML5-capable browser functionality to present terminal access, enabling users to interact with an internal Telnet host through the PCS web portal while retaining the clientless access model. Because the session is brokered through PCS and made available from the authenticated user portal, administrators can apply the resource-profile and role-based access controls associated with the Telnet resource.

These methods are specifically relevant to clientless terminal access because they deliver the terminal interface through the web-access workflow rather than requiring a separately deployed endpoint VPN client. Pulse Connect Secure describes its secure remote-access and clientless application-access capabilities in its Pulse Connect Secure data sheet; current product information is also available from Ivanti Connect Secure.

QUESTION NO: 11

Authentication Realms specify the authentication server, authentication policy, user directory/attribute store and what other element?

A. Radius Attribute Policy

B. Sign-in Notification

C. Role-mapping Rules

D. Authentication Protocol Set

ANSWER: C

Explanation:

Role-mapping Rules is correct because an Authentication Realm in Pulse Connect Secure combines the services that authenticate a user and retrieve that user's identity attributes with the rules that determine the user's authorization roles. After authentication succeeds, PCS evaluates role-mapping rules against the username and attributes obtained from the configured directory or attribute store. The matching rules assign one or more user roles, which in turn control the resources, bookmarks, access features, and policy settings available during the user's session.

This relationship is central to PCS access control design: the authentication server establishes identity, the authentication policy governs sign-in requirements, the directory supplies attributes, and role mapping converts those identity attributes into the roles used to enforce access. Realm-level role mapping can use criteria such as directory group membership, usernames, certificate fields, or other returned attributes, allowing administrators to grant access based on organizational identity data rather than manually configuring each user. Pulse Secure's administrator documentation describes Authentication Realms and their associated role-mapping configuration in the Roles, Realms, and Sign-In Policies guide.

QUESTION NO: 12

Which of the following are NOT required in an active/active cluster? (Choose two.)

A. A virtual IP address (VIP) configured on the PCS

B. An external load balancer

C. IP connectivity between nodes

D. All nodes having IP addresses in the same IP subnet

ANSWER: A D

Explanation:

An active/active PCS cluster distributes client traffic across multiple nodes through an external load balancer. Consequently, a virtual IP address does not have to be configured directly on PCS: the load balancer supplies the client-facing virtual service address and selects an available PCS node for each connection. PCS nodes retain their individual addresses for administration, node communication, and load-balancer health checks.

Also, active/active members do not have to reside in the same IP subnet. The architecture supports nodes in different network segments as long as the required network reachability exists between the cluster members and the load balancer can reach every node appropriately. This permits deployment flexibility, including placement of appliances in separate network zones when routing and relevant firewall rules allow the necessary traffic.

The external load balancer and inter-node IP connectivity are foundational to an active/active deployment because they enable traffic distribution and cluster communication. Pulse Secure's active/active clustering guidance describes the load-balancer-based topology and its network prerequisites. See the Pulse Connect Secure Active/Active configuration documentation and the Ivanti Connect Secure Administration Guide.