PassQueen
a.k.a dumpsqueen.com

Pulse Policy Secure (PPS) Deployment Implementation and Configuration

Pulse Secure PPS

Version Demo

Total Demo Questions: 15

Total Premium Questions: 153

Buy Premium PDF

https://passqueen.com

support@passqueen.com

QUESTION NO: 1

PPS supports policy enforcement devices.

A. False

B. True

ANSWER: B

Explanation:

True is correct. Pulse Policy Secure (PPS), now branded Ivanti Policy Secure, is a network-access-control platform designed to make access decisions and distribute enforcement information to network infrastructure. PPS evaluates endpoint posture, user identity, authentication context, and configured roles or policies. It can then work with enforcement devices such as Ethernet switches, wireless access infrastructure, firewalls, and other supported network devices to apply the access result. Depending on the integration and deployment design, enforcement can include assigning an appropriate VLAN, applying a role or access-control list, restricting a noncompliant endpoint, or allowing the endpoint to reach remediation resources.

This separation between policy decision and enforcement is central to PPS deployments: PPS determines what level of network access a user or device should receive, while the connected enforcement infrastructure implements that decision at the network edge. This allows an organization to consistently enforce access requirements across wired and wireless environments without relying on a single device to perform every policy function. Ivanti's official Ivanti Policy Secure product page describes its role in controlling access based on user and device context. Additional official product documentation is available through the Ivanti Help Center.

QUESTION NO: 2

PPS has which tools available to help troubleshoot

A. Telnet

B. Ping

C. Packet Walk

D. Traceroute

E. TCPDump

ANSWER: B D E

Explanation:

Pulse Policy Secure provides built-in network-diagnostic utilities that administrators can run from the appliance's troubleshooting interface to isolate reachability, routing, and packet-flow issues. **Ping** verifies basic IP reachability between PPS and a target host, helping confirm whether the appliance can communicate with DNS servers, authentication servers, gateways, or protected resources. **Traceroute** identifies the network path and hops used to reach a destination, which is useful for finding a routing break, an unexpected path, or excessive delay along the route. **TCPDump** captures packets observed by PPS interfaces for detailed analysis. A packet capture can validate whether requests arrive at PPS, whether replies leave it, and what protocol-level traffic is present during an access or connectivity problem. These tools are complementary: Ping establishes basic connectivity, Traceroute exposes the route, and TCPDump supplies packet-level evidence for deeper troubleshooting. PPS administration documentation groups these capabilities under troubleshooting and network-connectivity diagnostics. See the Ivanti Connect Secure Administration Guide and the Ivanti Connect Secure documentation portal.

QUESTION NO: 3

You must deploy VPN tunneling using Network Connect to multiple Microsoft Windows devices. Due to access restrictions, the users do not have permission to install WSAM. Which component resolves this issue?

A. Host Checker

B. third-party integrity measurement verifier

C. Windows Secure Application Manager scriptable launcher

D. Juniper Installer Service

ANSWER: D

Explanation:

Juniper Installer Service is correct because it is a Windows service designed to perform privileged installation tasks for Pulse Secure client components on behalf of users who do not have local administrator rights. In this deployment, Network Connect provides the VPN tunneling capability, while Windows Secure Application Manager is a separate endpoint component that may need to be installed or updated. Normally, installing such software requires elevated Windows permissions. With Juniper Installer Service installed and running on the endpoint by an administrator or software-distribution process, authorized users can initiate the required client installation through the PPS portal without being granted administrative access to the device.

This approach supports controlled enterprise rollout across multiple managed Windows endpoints: administrative privileges remain restricted, while the VPN workflow can still install the required WSAM component when policy or user access requires it. The service therefore addresses the stated access restriction without changing the users' Windows privilege level. For product documentation and current administration guidance, see the Ivanti Policy Secure Administration Guide and the Ivanti Product Documentation portal.

QUESTION NO: 4

Authentication false: radius answer with:

A. Radius challengue

B. Radius accept

C. Radius request

D. Radius reject

ANSWER: D

Explanation:

RADIUS Reject is the correct response when authentication fails. In the RADIUS protocol, a network access device or authentication client sends an Access-Request to the RADIUS server with the user's credentials. If the server cannot authenticate the user, or determines that the user is not authorized for the requested access, it returns an *Access-Reject* response. Pulse Policy Secure acts as a RADIUS client when it delegates authentication to an external RADIUS server, so a rejected authentication attempt is represented by this reject result. The reject response tells PPS that the authentication transaction did not succeed and that the user must not be granted a session based on that attempt. RFC 2865 defines Access-Reject as the message used when a request is denied and states that it may include a Reply-Message attribute to communicate an appropriate failure message to the user. This is the standard RADIUS behavior that PPS relies on when validating external authentication results. See the IETF's RFC 2865: Remote Authentication Dial In User Service (RADIUS), especially the Access-Reject definition, and Ivanti's Pulse Policy Secure RADIUS authentication documentation.

QUESTION NO: 5

Which three steps are required to add web compression to your existing ressources profile

(

A. Add the policy

B. Click show aLL autopolicy Types

C. Add the resource with the action set to compress

ANSWER: A B C

Explanation:

To enable web compression for an existing web resource profile, the required workflow is to add the policy, click “Show All AutoPolicy Types,” and add the resource with the action set to “Compress.” Web compression is configured as a resource policy action, rather than merely as a general property of the resource profile. Creating or adding the applicable policy supplies the policy container in which the compression rule is defined. Selecting “Show All AutoPolicy Types” exposes the available policy types, including the type needed to create a compression rule when it is not displayed in the default, filtered list. The administrator then adds the relevant resource entry and explicitly chooses the “Compress” action. This action instructs PPS to compress eligible HTTP content sent through the configured web resource, reducing transferred data for clients where the content and client capabilities support compression. The policy must be associated with the existing resource profile so that users who match the profile and policy receive the configured behavior. Pulse Policy Secure resource-profile and web-resource configuration is documented in the Pulse Policy Secure Administration Guide: Web Compression and the Resource Policies documentation.

QUESTION NO: 6

When a switch does not support 802. IX, the following should be used for port based enforcement

A. MAC auth

B. ARP

C. 802.1n

D. SNMP

ANSWER: D

Explanation:

SNMP is the appropriate method for port-based enforcement when the access switch cannot participate in IEEE 802.1X authentication. In this deployment model, Pulse Policy Secure communicates with the switch’s management plane through SNMP and applies the enforcement action to the physical port associated with the endpoint. Depending on the switch capabilities and configured enforcement policy, this can include changing the port’s VLAN assignment, disabling the port, or restoring normal access after the endpoint meets the required security posture.

This approach lets PPS extend access-control decisions to managed switches without relying on an 802.1X supplicant/authenticator exchange. For reliable operation, the switch must be reachable from PPS over the management network, SNMP credentials and version must be configured correctly, and the switch must support the relevant SNMP operations for port or VLAN control. IEEE describes 802.1X as port-based network access control, while SNMP provides the management interface used by compatible network devices for this alternate enforcement workflow. See the IEEE 802.1X overview and the Pulse Policy Secure technical documentation.

QUESTION NO: 7

Which two characteristics apply to policy Secure Demonstration and training edition (DTE) virtual appliances?

A. can you upgrade

B. only for lab

C. you can't add licenses

D. only 5 users

ANSWER: B D

Explanation:

“Only for lab” and “only 5 users” describe the intended use and capacity of a Policy Secure Demonstration and Training Edition virtual appliance. DTE is a non-production edition intended for demonstration, evaluation, training, and lab-style environments, rather than for deployment as an organization’s production access-control platform. Its purpose is to let administrators and learners configure policies, authentication, endpoint assessment, and access workflows in a limited environment.

The edition is also deliberately restricted to a maximum of five concurrent users. This limit makes DTE appropriate for demonstrations and small training exercises while distinguishing it from production virtual-appliance licensing, which is sized for operational user populations. When planning a PPS deployment, the administrator should therefore use DTE only to validate configuration and train staff, then select an appropriately licensed production appliance or virtual appliance for live service.

Ivanti’s Policy Secure documentation and product-support resources provide the applicable deployment and licensing guidance: Ivanti Policy Secure documentation and Ivanti Policy Secure support resources.

QUESTION NO: 8

How many seconds does it take to notify the fall of a node in a cluster?

A. 3

B. 5

C. 7

D. 1

ANSWER: B

Explanation:

5 is correct. In a Pulse Policy Secure cluster, member appliances exchange cluster health and status information so that a node failure can be detected and communicated promptly to the remaining cluster members. The expected node-failure notification interval is five seconds. This rapid notification supports cluster resiliency: once a peer is deemed unavailable, the cluster can update its view of active members and proceed with the applicable failover and session-handling behavior. The interval refers to notification of the node loss within the cluster, rather than the total time required for every dependent service, client connection, or external load balancer to complete its own recovery actions. Actual end-user recovery can therefore also depend on the deployment’s load-balancing, DNS, authentication, and session-persistence configuration. Pulse Policy Secure administrators should ensure that cluster members have reliable, low-latency connectivity for the cluster communication interfaces, because loss or degradation of that connectivity affects the health-monitoring mechanism on which failure notification relies. Consult the official Pulse Secure documentation portal and the Ivanti product documentation portal for the release-specific Pulse Policy Secure clustering and high-availability guidance.

QUESTION NO: 9

JTIC mode prerequisites

A. export the Trusted Server CAs

B. import the Trusted Server CAs

ANSWER: B

Explanation:

Import the Trusted Server CAs is the required prerequisite because PPS must possess and trust the certificate-authority chain that issued certificates for the servers involved in the JITC/JTIC deployment. Importing the Trusted Server CA certificates into the PPS trusted-server certificate store establishes the trust anchor needed when PPS validates a remote server's presented certificate. This validation confirms the server identity and helps ensure that protected authentication and access-control communications are established only with servers whose certificates chain to an approved authority.

The CA certificate, rather than merely an exported copy, must be installed on the PPS appliance before the relevant trusted-server connection can be validated. Administrators should obtain the appropriate root CA certificate and any required intermediate CA certificates, then import them in the certificate-management area of the PPS configuration. The resulting trust chain must be complete and current, including certificate validity dates and appropriate CA signing relationships. Ivanti's official Pulse Secure documentation resources are available through the Pulse Secure product documentation portal, and Ivanti's product documentation page provides supported documentation and release-specific guidance for certificate configuration.

QUESTION NO: 10

Which steps must you complete to configure a cluster?

A. Add IP Vip

B. Modify cluster propreties

C. Create cluster

D. Join cluster

E. Add member

ANSWER: B C D E

Explanation:

Configuring a Pulse Policy Secure cluster starts by creating the cluster on the initial appliance. This establishes the cluster identity and supplies the baseline configuration that participating nodes will use. The administrator then adds a member from the existing cluster configuration and completes the join operation on the appliance that is becoming a member. These are complementary parts of enrolling an additional PPS appliance: the cluster authorizes and identifies the member, while the new node connects to and joins the cluster.

After cluster formation, modifying cluster properties is part of completing the configuration. Cluster properties control shared operational settings and behavior for the cluster, including settings used to coordinate member operation and client access. A virtual IP address can be configured when a deployment requires a shared client-facing address and failover behavior, but it is a configurable cluster-access feature rather than a universally required, separately named step for every cluster configuration. Pulse Secure's administration documentation describes creating the cluster, adding and joining members, and configuring the cluster through its clustering administration workflow. See the Pulse Policy Secure Administration Guide and the Ivanti Product Documentation portal for the applicable PPS release documentation.

QUESTION NO: 11

What layer of the OSI model does SSL use?

A. Layer

B. Layer 7

C. Layer 8

D. Layer 2

E. Layer 6

ANSWER: E

Explanation:

Layer 6 is the correct answer. SSL, and its modern successor TLS, are conventionally associated with the OSI presentation layer because they provide security functions that transform application data before it is transported: encryption for confidentiality, integrity protection, and peer authentication through certificates. These services allow an application protocol such as HTTPS to exchange protected content without the application having to implement its own cryptographic record protection.

In practical TCP/IP networking, TLS is commonly described as operating between application protocols and TCP. This can make its placement seem less rigid than the seven-layer OSI teaching model. However, when an exam asks for the OSI layer associated with SSL, the expected conceptual mapping is the presentation layer, Layer 6, because that layer is responsible for data representation, encryption, and related transformations. The TLS specification defines the protocol's authentication, confidentiality, and integrity mechanisms, while the OSI model describes presentation-layer responsibilities including encryption. See the TLS 1.3 specification (RFC 8446) and IBM's OSI model overview.

QUESTION NO: 12

When device are profiled. Time stamps exist for: Chose 2 options

A. Last seen

B. Last updated

C. Last polled

D. First seen

ANSWER: A D

Explanation:

Device profiling records lifecycle-oriented discovery timestamps that show when PPS first identified an endpoint and the most recent time it observed that endpoint. **First seen** is the initial discovery time retained for the profiled device. This value is useful for establishing when the device first entered the profiling database and for investigating the history of newly introduced endpoints.

Last seen is refreshed when PPS subsequently observes the device. It lets administrators determine how recently the endpoint was present or detectable on the network, which is valuable when reviewing endpoint inventory, validating ongoing device activity, and investigating access events. Together, these two timestamps provide the beginning and most recent observation points for a device profile, rather than a general record of every configuration or polling activity.

PPS administrative documentation and product resources describe the endpoint and device-management capabilities used to view and manage discovered devices. See the Ivanti Policy Secure Administration Guide and the Ivanti Product Documentation portal for the applicable release-specific interface details.

QUESTION NO: 13

Cloud secure supported platforms

A. macOS

B. iOS

C. Windows

D. Chrome OS

E. Android

ANSWER: A B C D E

Explanation:

Pulse Secure Cloud Secure is designed to provide secure access from the common endpoint operating systems used by organizations and mobile users. The supported-platform set includes macOS and Windows for desktop and laptop endpoints, plus iOS and Android for mobile devices. Chrome OS is also supported, enabling Chromebook users to access protected resources through the applicable Pulse Secure client and browser-based secure-access capabilities. Together, these platforms allow an organization to apply a consistent secure-access service across managed and personally owned endpoints while accommodating the major desktop, mobile, and Chromebook ecosystems. Platform support still depends on the applicable client version, operating-system release, authentication configuration, and any features enabled by the Cloud Secure tenant. Administrators should therefore verify the client and OS compatibility requirements before deployment, particularly when planning device upgrades or using advanced endpoint-security checks. Pulse Secure product information and support resources are available from Pulse Secure Connect Secure and the Ivanti Secure Access documentation portal.

QUESTION NO: 14

You are deploying a VPN tunneling client and are asked to configure a restrictive set of tunneling policies. In the Admin UI, which two VPN Tunneling role settings apply? (Choose two.

A. Split Tunneling

B. Connection Settings

C. VPN Tunneling Access Control

D. Route Monitor

ANSWER: A C

Explanation:

Split Tunneling and **VPN Tunneling Access Control** are the role settings used to establish a restrictive VPN-tunneling policy. Split tunneling controls the destination traffic that the Pulse client sends through the secure tunnel. An administrator can define included networks so that only traffic intended for approved internal destinations is routed into the VPN, rather than allowing broad access through a full tunnel or permitting unrestricted route selection.

VPN Tunneling Access Control applies policy enforcement to traffic traversing the tunnel. It lets the administrator define permitted source, destination, protocol, and port combinations for a role, enabling least-privilege network access after the user has successfully connected. Used together, these settings constrain both the routing scope of tunneled traffic and the services that the assigned role can reach.

These controls are configured in the VPN Tunneling area of a user role, so they can be applied consistently according to authenticated role membership. Ivanti's Pulse Policy Secure documentation describes user-role configuration and VPN tunneling policy features in the Pulse Policy Secure Administration Guide. Product documentation is also available from the Ivanti Product Documentation portal.

QUESTION NO: 15

How many members in active-standby cluster

A. 3

B. 2

C. 4

D. 1

ANSWER: B

Explanation:

2 is correct. A Pulse Policy Secure active-standby cluster consists of a pair of PPS appliances: one node operates as the active member and processes user traffic, while the other operates as the standby member. The two members synchronize the required configuration and session-related cluster state so that the standby appliance can assume the active role if the active appliance becomes unavailable. This two-node design provides high availability without requiring users to select a different gateway manually after a node failure.

In PPS clustering terminology, active-standby is specifically a redundancy pair, rather than a multi-member load-balancing architecture. During normal operation, only the active node provides service for the cluster's virtual IP address; the standby node monitors the active peer and is prepared for failover. Deployment planning must therefore include two compatible PPS nodes, appropriate network connectivity between them, and a shared cluster configuration. Pulse Secure's administration documentation describes clustering and the active/standby high-availability model in its PPS administration guidance. See the Pulse Policy Secure Administration Guide and the Ivanti Product Documentation portal for the applicable release documentation.