Pulse Secure®

Cloud Secure Brief

Hemanth Kumar K

Cloud Secure

Cloud Secure, functionality built into Pulse Connect Secure (PCS), provides secure access to enterprise resources on a hybrid IT environment where companies are combining the best of the cloud with their own localized data center

Key features of Cloud Secure

1. **Secure Single Sign-On (SSO)** – Cloud Secure supports SAML based SSO which allows preauthenticated users to access resources without entering credentials again for applications which are accessed. It also tunnels authentication exchanges between client and PCS thus providing Secure Single Sign-On to SaaS, Cloud, and Enterprise hosted resources.

2. **Compliance** – Cloud Secure leverages Pulse Secure's Host Checking capabilities in desktops and MDM device attributes in mobile devices to give best in class compliance posture assessment capabilities and allows for varying levels of access based on device compliance and well as user-based information.

3. **Certificate authentication** - Certificate authentication eliminates the need for users to provide credentials manually every time On-demand VPN is triggered.

4. **On demand VPN/Location based VPN** - Automatic VPN connection, based on location through Pulse client in Desktops and through On-demand VPN support in mobile devices eliminates users triggering manual VPN connections.

5. **Split Tunneling** - Cloud Secure eliminates data center hair pinning (also known as back hauling) by optionally only sending authentication, authorization, and compliance check traffic to PCS and sending application data directly to the cloud.

6. **Role Based Access Control** (RBAC) – RBAC allows access to resources based on the roles assigned to users.

7. **Compliance failure notification** – Cloud Secure supports notifications for Compliance failure scenarios. A remediation notification helps notify end users about the reason of failure and the necessary steps to get the device into a compliant state.

8. **Better integration with Mobile Device Management (MDM) servers** - Cloud Secure integration with MDM servers helps in better management of mobile devices by keeping the corporate data secure from personal data. In addition to this, better compliance rules and enforcement methods are possible with device attributes retrieved from MDM servers.

9. **Extensible Identity Management** - Cloud Secure integrates well with Third-Party Identity Providers to support existing customer deployments that have already implemented these Identity management solutions.

10. **On-Premise Cloud access** – Cloud Secure supports SSO for on-premise users authenticated to Pulse Policy Secure (PPS). This is done by sharing session information from PPS to PCS through IF-MAP federation and removes the need to establish a VPN tunnel directly to PCS.

11. **Simplified and Redesigned Administrator Experience and Interface** - Cloud Secure configuration possible through a simplified and intuitive admin interface. These improvements enhance the admin experience and helps them by prepopulating the relevant settings, reuse existing configurations and guide them with insightful help sections.

User Experience

Cloud Secure is designed to provide seamless user experience across mobile devices and desktops. Cloud Secure gives better user experience by using features like Certificate authentication, location awareness and On demand VPN for session establishment. This eliminates multiple passwords across different services, and the VPN connection can be configured to auto launch when the user accesses an application.

Mobile Devices

When a user launches a MDM managed application, the VPN connection can be configured to automatically launch. Certificate authentication is used to authenticate the user and VPN connection will be established after compliant posture assessments through MDM retrieved attributes.

Once the application is launched, User has to enter his username or enterprise domain (based on the application). Existing VPN session will be re-used for generating SAML assertions and User gets access to the applications.

Desktops

In desktops, an end-user can either manually connect to VPN or connect automatically through Location awareness rules. Re-use of existing VPN/IF-MAP session provides the Single Sign-On experience.

It is recommended to use credential provider based authentication or Location awareness rules to auto launch VPN connections to get the best user experience with Cloud Secure Single Sign-On

Note: When configured to do so, Cloud Secure eliminates passwords, auto launches VPN connections and handles all the technical intricacies in the backend such that user gets Secure Single Sign-On in one touch

Understanding Cloud Secure and SAML

Cloud Secure uses Security Assertion Markup Language (SAML) for the exchange of authentication information between client device (Mobile devices & Desktops), Service Provider (Cloud applications like Office 365, Salesforce etc.) and Identity Provider (Pulse Connect Secure) to provide SSO. Single Sign-On, using SAML, is classified into IdP initiated and SP Initiated sessions.

- In SP initiated scenario, when the end user tries to access the application, the cloud service triggers SAML authentication requests and redirects them to IdP for authentication.
- In IdP initiated scenario, user first authenticates with Identity provider before accessing the cloud service.

Fully Qualified Domain Names (FQDNs)

SAML implementation in PCS uses Host FQDN and Alternate Host FQDN for communicating with external cloud applications. DNS resolution of these FQDNs is key in achieving SSO. Typically, enterprises have internal DNS servers for resolving internal resources.

The following table outlines how and why the DNS resolution of SAML FQDNs affects SSO.

DNS resolution with VPN	DNS resolution without VPN
Host FQDN should resolve to external port ip of PCS. Once the VPN session is established, client looks up internal DNS servers first, and resolves alternate host fqdn to internal port ip. This helps in reusing the existing VPN session to provide Single Sign-On	Both the Host FQDN and Alternate host FQDN resolve to external port ip. This is to ensure that users get access to cloud services even without VPN connection. This allows the SAML requests to reach PCS

Note: Public DNS servers should resolve Host FQDN and Alternate Host FQDN to external port IP Address of PCS. Internal DNS servers should resolve Alternate host FQDN to internal interface IP Address

SAML settings

The key PCS SAML URLs used in Service provider configurations are:

- Entity ID: https://<HOST FQDN of PCS>/dana-na/auth/saml-endpoint.cgi
- SAML Sign-in URL (SSO URL): https://<AlternateHost FQDN>/dana-na/auth/saml-sso.cgi
- Enhanced Client or Proxy (ECP) URL: https://<HOST FQDN of PCS>/dana- na/auth/samlecp.ws

Certificate Requirements

Cloud Services(SP) SAML configuration requires SAML Sign-in URL or Redirect URL of Identity Provider(PCS). All the authentication requests from Service Providers gets redirected to this URL. SAML Sign-In URL of PCS is

https://<Alternate Host FQDN>/dana-na/auth/saml-sso.cgi.

Note: Alternate Host FQDN is used in SAML Sign-in URL

VPN connection is always established to Host FQDN of PCS and the SAML authentication requests are redirected to Alternate Host FQDN. So, PCS should have certificates to trust and allow connections to both Host FQDN and Alternate Host FQDN.

Note: Cloud Secure requires either Wild Card certificates or Subject Alternative Name certificates (includes all SAML FQDNs). This is to trust and allow connections to all the SAML FQDNs

Compliance Check

Compliance checks for desktop

Cloud Secure supports compliance for Windows and Macintosh desktops/laptops through Pulse Secure's rich Host Checking capabilities. Admins can leverage the existing custom and pre-defined checks to configure multiple rules across platforms and allow only compliant users/devices to access Cloud resources. Continuous monitoring of endpoints and dynamic policy evaluations helps in revoking access immediately when the endpoint goes out of compliance.

Note: If Split tunneling is enabled on PCS, then client sends only authentication/authorization data through PCS and all the application data directly to cloud. In such cases, users may get extended access to services even after going out of compliance, until the session expires in the cloud application

Compliance checks for mobile devices

Cloud Secure supports compliance checks for mobile devices through MDM servers. MDM servers get all the device attributes from the mobile devices during registration and keeps updating them through continuous monitoring and polling.

PCS retrieves mobile device attributes from MDM servers during mobile user authentication/authorization. Admin can use these attributes to define relevant role mapping rules to allow access to only compliant devices.

Cloud Secure mandates admins to configure on demand vpn for all the mobile applications. This helps in automatic trigger of VPN connections whenever managed application is accessed. This helps in performing compliance checks every time VPN connection is triggered.

Note: Alternate Host FQDN is used in SAML Sign-in URL

Limitations

Compliance check happens during VPN connection establishment. Continuous compliance checks are not supported in mobile devices.

On-Premise use case

Cloud Secure provides Single-sign on access to cloud services for on-premise users authenticated to PPS after compliance posture assessments. On premise users are authenticated by PPS when they are connected to enterprise network. PPS exports this session to Federation server through IF-MAP federation capability. PCS acts as Federation client and imports session information from Federation Server and uses this imported session information to generate SAML assertions to provide access to On-Premise users. This eliminates users providing credentials again with every application access.

Advantages

One of the advantages of this model is that, only one user license is consumed and users from multiple sites connected to multiple PPS servers can federate the session to PCS IdP thus providing SSO for compliant users across the enterprise.
Compliance check for on-premise users is performed by **PPS**.

- In desktops, Host Checker in PPS does the configured/relevant checks before giving access.
- In mobile devices, PPS retrieves the mobile device attributes from MDM servers and does compliance assessments before giving access.

Limitations

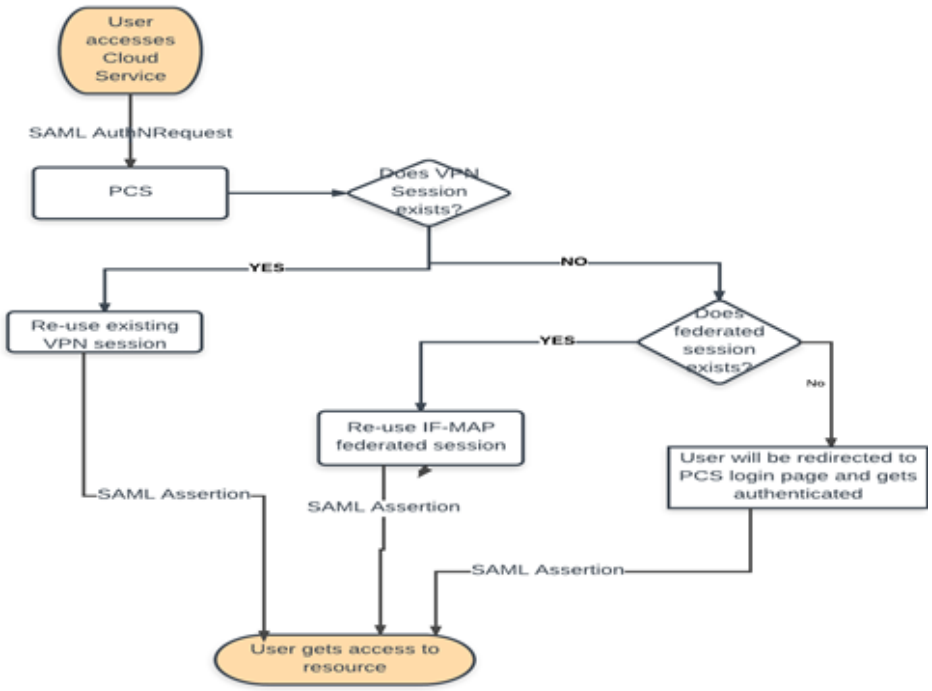
Cloud Secure 'IF-MAP session reuse' uses endpoint ip as the identifier. Because of this,

1. This solution does not work if there is a NAT device between endpoint and PPS.
2. RADIUS accounting should be enabled for pure L2 sessions. This helps in updating the IP information in PPS session.

Re-use order

Cloud Secure Single Sign-On is achieved through reuse of existing sessions. Below flow chart explains the re-use logic implemented in PCS.

Note: The key to Single Sign on is Re-use of existing session. This is achieved either from existing VPN session for remote users or through IF-MAP federated session from PPS for the on-premise users



Third Party Support

Cloud Secure is a comprehensive solution from Pulse Secure aims at providing Secure Single Sign-On to users across multiple client platforms (iOS, Android, MAC, Windows), for various cloud services. The solution is achieved using Pulse Secure Access Suite comprising Pulse Connect Secure, Pulse Policy Secure, Pulse Workspace. In some cases, customers would have already deployed MDM, IdP servers from different vendors. To address these deployments, Cloud Secure integrates well with Third-Party products from different vendors and helps customers for a seamless integration and faster deployments with minimal changes.
Note: Cloud Secure supports integration with MobileIron and AirWatch MDM servers

Understanding IdP Federation with Cloud Secure

SAML enables cloud services to delegate Authentication to an Identity provider. However, sometimes one Identity provider can delegate authentication to another Identity provider. This mechanism is called **IdP federation**.

Note: Cloud Secure supports integration with MobileIron and AirWatch MDM servers

For the rest of this section, consider OKTA as the third-party Identity provider delegating Authentication requests to Cloud Secure. In this federated solution, OKTA acts as both Identity Provider (for Cloud services) and Service Provider (for Pulse Connect Secure). Inbound SAML capabilities of Okta allows users to authenticate to Okta using Pulse Connect Secure as external SAML Identity Provider to enable Secure Single Sign-On to Cloud applications.

As an example, let say Zendesk can delegate authentication to OKTA (IdP #1). However, OKTA in turn delegates authentication to Cloud Secure (IdP #2). In such a case, a chain of authentication looks like:

Advantages

This helps the customer to get the additional benefits of Cloud Secure such as compliance checks, Secure Single Sign-On through VPN tunneling. In addition to this, minimal changes are required to integrate PCS IdP in the existing SAML deployments and helps in faster deployments.

Pulse Secure®

Corporate and Sales Headquarters
Pulse Secure LLC
2700 Zanker Rd. Suite 200
San Jose, CA 95134
(408) 372-9600
info@pulsesecure.net
www.pulsesecure.net

ABOUT PULSE SECURE

Pulse Secure, LLC offers software-defined Secure Access solutions that provide visibility and easy, protected connectivity between users, devices, things and services. The company delivers suites that uniquely integrate cloud, mobile, application and network access control for hybrid IT. More than 23,000 enterprises and service providers across every vertical rely on Pulse Secure to empower their mobile workforce to securely access applications and information in the data center and cloud while ensuring business compliance. Learn more at www.pulsesecure.net.

linkedin.com/company/pulse-secure
www.facebook.com/pulsesecure1
twitter.com/PulseSecure
info@pulsesecure.net

VERSION 022920