Every day, Juniper Networks is helping our customers build the best networks on the planet. Every innovation we envision, every technology we create is informed by our desire to help solve our customers’ toughest challenges so they can compete and thrive today and into the future.

SecureAuth IdP & Juniper Networks

Pulse Secure, formerly a part of the Juniper Networks’ SSL VPN product line, enables secure access from any device to enterprise apps and services in the data center or cloud. To provide a secure connection to protected resources, the highly-configurable and extremely flexible SecureAuth IdP can be integrated with the Juniper IVE product to authenticate remote end-users.

SecureAuth IdP integrates with third-party products to enable a VPN (Virtual Private Network) connection between a network and computer for end-users physically located outside of an organization. An SSL (Secure Socket Layer) VPN protocol used with SecureAuth IdP creates a secure HTTPS session from a PC web browser to the application server being accessed. Additional software is not required since the web browser is used as the client application.

The end-user submits credentials via a VPN client which contacts the VPN server to authenticate and connect the remote user to the internal network. The VPN connection employs strong encryption for the end-user’s access to restricted, private data, thereby keeping this data secure from the other users of the underlying network, which might be a public network such as the Internet.

The Juniper Networks / Pulse Secure product is an SSL VPN that establishes a secure remote access tunnel into the network and corporate resources, creating a protected access path to sensitive data. When integrated with Juniper IVE, SecureAuth IdP enables 2-Factor Authentication or Single Sign-on (SSO) access via SAML 1.1 or 2.0, X.509 Certificate Delivery, or RADIUS for end-users authorized to connect to the remote network via SSL VPN.

Using SAML, the assertion can be configured to be initiated by the Service Provider or by SecureAuth IdP. Juniper IVE can also be configured as the Identity Provider to authenticate users and issue a SAML assertion to SecureAuth IdP which would function as the Service Provider. Or SecureAuth IdP can be configured to enable SSO access via SAML to Juniper IVE VPN.

Additionally, Juniper IVE VPN can be configured to provide the SSL service for SecureAuth IdP, in a setup with a wildcard SSL certificate installed on Juniper IVE.

For certificate-based authentication scenarios, SecureAuth IdP enables easy certificate enrollment that does not require any manual or tedious labor for the customer. The user can securely enroll for a certificate before attempting access to Juniper, or Juniper can redirect users to SecureAuth IdP if a valid certificate is not present at login. Once the certificate is acquired, users can access Juniper and its protected resources based on its established trust with SecureAuth IdP (through certificates).

SecureAuth IdP can also act as a RADIUS Server, authenticating users via the RADIUS protocol to securely enable access to a RADIUS Client (Juniper, for example).
Integration Guides

- Juniper IVE (IdP-initiated) Integration Guide (SAML 2.0)
- Juniper IVE (SAML 1.1) Integration Guide
- Juniper IVE (SP-initiated) Integration Guide (SAML 2.0)
- Juniper IVE as the SAML IdP to SecureAuth IdP Integration Guide
- Juniper IVE Single Sign-on Configuration Guide (SAML)
- Juniper IVE Virtual Hostname Configuration Guide
- Juniper Pulse iOS Provisioning Integration Guide (Certificate)
- Juniper SSL VPN Integration Guide (RADIUS)