Pulse Secure®

Pulse Connect Secure

Overview

Enterprises and service providers have the difficult challenge of providing location- and device-independent network connectivity that is secure and capable of controlling resource access for authorized users. Breaches and threats continue to spiral out of control and increasing numbers of employees and users want to use their own personal productivity solutions.

Pulse Connect Secure provides secure, authenticated access for remote and mobile users from any web-enabled device to corporate resources—anytime, anywhere. It is the most widely deployed SSL VPN for organizations of any size, across every major industry.

Pulse Connect Secure includes Pulse Secure Clients, which are dynamic, multiservice network clients for mobile and personal computing devices. Pulse Clients are simply deployed, enabling users to quickly "click and connect" from any device, anywhere. Pulse Secure mobile clients deliver per–application SSL VPN connectivity for iOS and Android platforms, enabling IT to create an even more transparent and secure mobile app experience for their users.

Pulse advantages:

Securing and streamlining access to data center and cloud – anywhere, anytime

Per-app and on-demand application access means data is secured, and workers are more productive

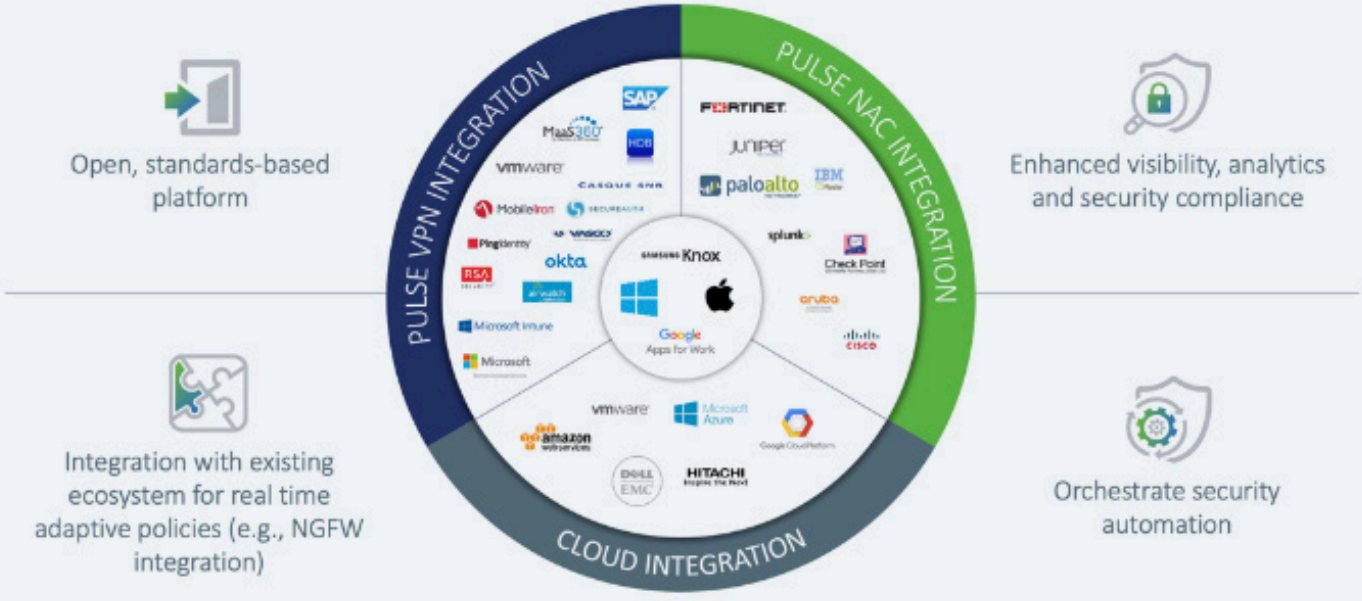
- Clientless access – Access web applications and virtual desktops with nothing to install
- Robust Policy Engine – Pulse Secure's Role based policy framework allows defining granular and conditional access policies to control user access to corporate resources
- Strong authentication – Support for MFA, SAML 2.0, PKI, IAM, built-in TOTP, biometric auth for mobiles and digital certificates
- Stateful Host Checker – Check remote devices for security compliance before and throughout the session
- Unified client – Single client for multiple use cases (VPN, NAC, ZTA) and supports seamless access and delightful user experience supported across all major OS platforms
- MDM Integration – support for 3rd party solutions to enable enhanced policy enforcement
- Single sign-on (SSO) – simplify access with SSO to data center and cloud
- Centralized Management –Pulse One platform enables centralized management of policy, compliance, and authorization for cloud and data center access
- Optional 3rd party integrations – Integrates with AirWatch and MobileIron for EMM and many IDPs

Key Functionality:

FEATURE	FEATURE DESCRIPTION
Layer 3 SSL VPN	• Dual-transport (SSL + Encapsulating Security Payload) full Layer 3 VPN connectivity with granular access control. • "Always on VPN" & "VPN Only Access" modes for Compliance.
Application VPN	• Client/server proxy application that tunnels traffic from specific applications to specific destinations (available for Windows devices only). • "On Demand VPN" and "Per App VPN", for seamless & secure end user experience.
Clientless Core Web Access	• Enables browser-based access with integrated content intermediation engine to provide secure access to web applications
Single Sign-On	• Pulse Secure supports plethora of SSO of protocols like SAML, Kerberos, Kerberos Constrained Delegation, NTLM, Form-Post SSO to provide seamless sso access to enterprise resources in Hybrid IT
Optimized end-user experience	• Smooth roaming from remote access to local LAN access (Pulse Policy Secure). Single Sign On (SSO) for rapid, secure access from remote or onsite locations (via integration with Pulse Cloud Secure and Pulse Policy Secure)
AWS, Azure and Alibaba cloud Support	• Available on Amazon Web Services, Microsoft Azure and Alibaba clouds. Dedicated installation guides are downloadable on the Pulse Secure Technical Publications website.
Stateful endpoint integrity and assessment	• Assess and remediate end user devices prior to authentication with easy policy definition. •" Windows 10 (Desktop & Mobile), Mac OS X, Apple iOS, and Android.
Layer 7 Web single sign-on (SSO) via SAML	• Allows end users to authenticate to the network through a Layer 3 tunnel, while simultaneously enjoying SSO to Web applications accessed through their browser via SAML SSO support.
Split tunneling options	• Allows full range of split tunneling options, including support for individual IP addresses as well as FQDN.
Flexible launch and connectivity options	• Users can easily launch SSL VPN via their Web browser, or directly from their desktop • Auto Connect feature allows devices to automatically connect to VPN, either at the time when the machine starts or user logs on. • VPN on demand and location awareness allows auto triggering VPN, seamlessly in the background, when an approved application or endpoint needs corporate access.
Pulse Cloud Secure	• Pulse Connect Secure can act as SAML Identity Provider and extends Secure and Compliant access capabilities to SaaS applications
Preconfiguration options (Windows and Mac only)	• Administrators can preconfigure a Pulse Secure deployment with a list of gateways for end users to choose from
Authentication options	• Administrators can deploy Pulse Secure for remote user authentication using a wide array of authentication mechanisms, including hardware token, smart card, soft token, Google Authenticator, RSA SecurID, Duo, one-time passwords, one-time passwords and certificate authentication. • SAML authentication, for delegating user authentication to an Identity Provider.

RDP/Telnet/SSH sessions using HTML5	• 100% clientless access using HTML5 browsers.
VMware Horizon and Citrix XenApp/ XenDesktop VPN	• Pulse Secure supports the latest versions of VMware and Citrix. For specific details, consult our Supported Platforms Guide available at www.pulsesecure.net/techpubs
Granular SSL Cipher Configuration	• Enables the administrator to select specific ciphers over those pre-configured for highly secure compliance.
REST API	• A comprehensive REST-based API for programmatic access to the appliances for regular maintenance or policy enforcement operations. You can set commands or expose configuration retrieval, aiding in automation and orchestration.
Standard based built-in Time-based-One-Time Password (TOTP)	• Leverage smart phones to roll out a cost-effective and self-serve two-factor authentication mechanism, where one-time passcodes are generated by a mobile app implemented based on RFC6238
Adaptive MFA	• On successful primary authentication, Adaptive MFA creates an overall risk profile with user, device, and location behavior to determine if a secondary authentication challenge should be issued prior to session creation.
Multiple Tunnels	• Pulse Secure's unified client can establish multiple tunnels to different PCS gateways simultaneously, both on-premise and in the cloud. This ensures that users can access all applications protected by different gateways simultaneously without switching between gateways to access applications in different locations.
MDM Integration	• Integrates with third party MDM solutions to gain comprehensive endpoint visibility and support additional mobile use cases. Supports vendors like AirWatch, MobileIron, Microsoft Intune in addition to Pulse Workspace
SSL VPN federation with NAC	• Seamlessly provision SSL VPN user sessions into NAC sessions upon login. This enables users to roam from on-prem and remote locations with a single login and seamlessly access corporate resources.

Integration Into Existing Ecosystem



Ordering Options:

PSA Series Appliance Family Ordering Information

PSA Series Appliance Family Licensing Options

Model Number	Description*
PSA Series Appliances	
PSA300	PSA300 Appliance for SSL VPN users or NAC users. Supports up to 200 SSL VPN or 500 NAC concurrent user sessions. .
PSA3000	PSA3000 Appliance for SSL VPN users or NAC users. Supports up to 200 SSL VPN or 500 NAC concurrent user sessions.
PSA5000	PSA5000 Appliance for SSL VPN or NAC users Supports up to 2,500 SSL VPN or 10,000 NAC concurrent user sessions.
PSA7000	PSA7000 Appliance for SSL VPN or NAC users Supports up to 25,000 SSL VPN or 50,000 NAC concurrent user sessions.
PSA-V Series Appliances	
PSA3000-V	Supporting 2 vCPU cores and up to 200 VPN / 500 NAC concurrent sessions.
PSA5000-V	Supporting 4vCPU cores and up to 2500 VPN / 10K NAC concurrent sessions
PSA7000-V	Supporting 8 vCPU cores and up to 25K VPN / 50K NAC concurrent sessions
Ordering Number	**Description***
Connect Secure Licenses	
CONSEC-xU(-zYR)	Add x simultaneous PCS users to Pulse PSA Appliance (x options: 10, 25, 50, 100, 250, 500, 1000, 2000, 2500, 5000, 7500, 10K, 15K, 20K, or 25K concurrent sessions) Subscription Licenses (z options: 1, 2, or 3 year).
CONSEC-ADD-yU	Add y simultaneous PCS users to Pulse PSA Appliance (y options: 10, 25, 50, 100, 250, 500, 1000, 2000, 2500, 5000, 7500, 10K, 15K, 20K, or 25K concurrent sessions) Perpetual for hardware platform where activated.
Leased Licensing Licenses	
ACCESS-LICENSE-SVR	Enables enterprise access appliance as a license server.
PSA-LICENSE-MBR	Allows PSA appliance to participate in leased licensing.
ICE (In Case of Emergency) License Options	
PSA-ICE	In Case of Emergency (ICE) license for PSA Series Appliance.
Java RDP (Remote Desktop Protocol) Applet License Options	
ACCESS-RDP-xU-zYR	Java RDP Applet z-Year subscription for x simultaneous users (x options: 50, 100, 250, 500, 1,000, 2,000, 2,500, 5000, 7500, or 10K simultaneous users. RDP user license count cannot exceed the number of user licenses) (z options: 1, 2, or 3-year subscription).

Hybrid IT Checklist

	Data Center						IaaS	
	 Physical Appliance			 Virtual Appliance			 Cloud	
		VPN	NAC		VPN	NAC		VPN
Models and License Capacity	PSA300/3000 PSA5000 PSA7000	200 2500 25000	500 10000 50000	PSA3000-V PSA5000-V PSA7000-V	200 2500 10000	500 10000 50000	PSA3000-V PSA5000-V PSA7000-V	200 2500 25000
Platforms	Purpose-built			VMware, KVM, Hpyer-V			Azure, AWS	
Supported Software Services	VPN, NAC			VPN, NAC			VPN	
Software Licensing	Perpetual, Subscription			Subscription			Subscription	
Clustering	Active / Active Active / Passive			Active / Active Active / Passive (Limitations: 2 node, VMware)			Planned	
ICE (In Case of Emergency)	✓			✓			✓	
License Server (on-premises)	✓			✓			✓	

Pulse Secure®

咨询订购：400-010-8885、 Support@PulseSecure.global

咨询订购：400-010-8885、 Support@PulseSecure.global