Pulse Secure®

PRODUCT BULLETIN

PULSE CONNECT SECURE, PULSE POLICY SECURE AND PULSE CLIENT UPDATES FOR 9.1R1

Bulletin Date

May 2019

Applicable to All Regions

Effective Change Date

May 2019

Introduction

Today's digital era is challenging workforce productivity, from the 9-to-5 workdays to means of accessing and digesting data. More importantly, access to data and applications across different mediums, mobile to cloud, are redefining traditional IT processes and policies. Pulse Secure has made it easier to secure your data center, provide mobile access and enable new cloud services with our integrated Secure Access Solution. This Product Bulletin describes new features and functions available in the 9.1R1 release of Pulse Connect Secure, Pulse Policy Secure, and the Pulse Secure Desktop Client.

These new releases from Pulse Secure enable network administrators to expand their secure access solution support for network performance and security.

This release focuses on Secure Access for IoT devices, Provisioning PCS sessions to Check Point Firewall using IF-Map through PPS and Cloud Application Visibility. Also, Pulse Desktop Client and Host Check support is added for the 64-bit macOS.

What’s New

Common Features for Pulse Connect Secure and Pulse Policy Secure

Key Feature	Benefit
• Ability to send DNS traffic on any interface	• When PCS is deployed on virtual/cloud environments, there is very likely chance that DNS infra is accessible from external interface. Hence, PCS now provides capability to specify which interface to use for DNS traffic.
• Authentication failure management	• Account Lockout option to manage user authentication failures for admin users of local authentication server. The admin user account will be locked after specified number of consecutive wrong password attempts. The account will be unlocked after the specified lockout period or by using the Unlock option.
• Deploying PSA-V in KVM	• User can deploy PSA-V in Kernel-based Virtual Machine using a template.

Pulse Connect Secure 9.1R1

From 9.1R1 release onwards, Pulse Secure is introducing Pulse Secure Software Defined Perimeter. It provides tight integration to build a simple and powerful solution with PCS, PPS, vTM and Pulse One all-together. For detailed information on SDP, refer to the following SDP documents on https://ww.pulsesecure.net/techpubs.

- SDP Release Notes
- SDP Supported Platforms Guide
- SDP Getting Started Guide
- SDP Deployment Guide

The following table lists the non-SDP features for Pulse Connect Secure 9.1R1.

Highlighted Features in this Release

Key Feature	Benefit
• Pulse SAM IPv6 support	• PCS now supports IPv6 traffic over Pulse SAM on Windows 10/8.1/7.
• snmpget for monitoring VLS and Max Users	• PCS now supports the ability to retrieve maximum number of licensed users using snmpget.
• Mac NPAPI Deprecation fix	• On Mac platform, NPAPI is deprecated. PCS now provides ability to launch all Pulse clients on Mac using PSAL component.
• User access to internet resources on an Azure-based or AWS-based PCS	• AWS VPC and Azure VNet gateways drop packets if the source IP is the endpoint tunnel IP. This feature NATs endpoint tunnel IP to Internal interface IP. The NAT allows users to access internet resources when connected to a VPN tunnel on an Azure or AWS-based PCS.
• REST API enhancements	• Enhancements include: ▪ Getting Config without Pulse packages such as ESAP package and Pulse Client package ▪ Backing up and restoring binary configuration
• Support for “client-name” parameter in HTML5 Access	• User can pass "client-name" in HTML5 rdp using launcher method. The %clientname% variable is matched with a workstation ID and normally that variable is unique and dedicated remote desktop computer name.

Cloud Secure Specific Features in Pulse Connect Secure 9.1R1

Highlighted Features in this Release

Key Feature	Benefit
• ECP Throttling	• ECP throttling provides a mechanism to identify and stop all duplicate ECP requests being sent to AD server for authentication thus preventing the user from AD account lock out.

Pulse Policy Secure and Profiler 9.1R1

Highlighted Features in this Release

Key Feature	Benefit
• SNMP Enforcement using ACL (Cisco, HP, Juniper)	• An alternative solution for 802.1x enforcement implementation where it enables administrator to easily deploy L2 enforcement where some switches does not support RADIUS capability.
• SAML Authentication support with PPS	• SAML Server support on Pulse Policy Secure (PPS) enables users to get authenticated to PPS using SAML Identity Providers like PCS, Ping, Okta and apply Layer2 or Layer3 access control.
• Google TOTP Auth Server support	• Enable administrators to use cost-effective Google (TOTP) Time based One-Time Password authentication as a secondary authentication.
• Session Migration using Cert auth	• Enable users to authenticate using Certificate and provide seamless session migration from PCS to PPS without entering additional user credentials.
• TACACS+ Enhancements – Config sync, TACACS+ Client import, custom attributes support for Juniper and F5 devices.	• Enables administrator to migrate TACACS+ clients from other solution to PPS. Provide redundancy via config syn across WAN link and custom TACACS+ attribute support for Juniper and F5 during authorization request.
• Meraki 802.1x & Guest Access support	• Provide 802.1x and Guest management solution with Cisco Cloud managed Meraki wireless networks.
• WAN cluster support (Config Only)	• This feature supports config-only Active/Active WAN Clustering in PPS for multi-site deployments with clustering across WAN link.
• Distributed Profiler with bi-directional sync	• In distributed environment, this feature enables administrators to use remote office with Profiler forwarder functionality along with local profiler and PPS capability on the same appliance. It enables Profiler data sync over WAN link (e.g. Between Main Data Center and Disaster Recovery)
• Profiler Devices age out	• This feature provides admin the capability to define the Age of devices, after which they get deleted from database and efficiently managed Profiler device license consumption.
• Agentless Host Checking – additional AV support	• Enhanced security posture with additional AV product support via agentless host checking (MacAfee Endpoint Security 10.x, Trend Micro Maximum Security 15.x, Sophos Home 15.x, Avast Enterprise and Norton Enterprise).

Pulse Secure Desktop Client 9.1R1

From 9.1R1 release onwards, Pulse Secure is introducing Pulse Secure Software Defined Perimeter. It provides tight integration to build a simple and powerful solution with PCS, PDC and Pulse One all-together. For detailed information on SDP, refer to the following SDP documents on https://www.pulsesecure.net/techpubs.

- SDP Release Notes
- SDP Supported Platforms Guide
- SDP Getting Started Guide
- SDP Deployment Guide

The following table lists the non-SDP features for Pulse Desktop Client 9.1R1.

Highlighted Features in this Release

Key Feature	Benefit
• Launching Pulse Desktop Client using URL	• Pulse Desktop Client can now be launched using a URL. Customers can insert the URL in any tools (For example: Support ticket management tool), so that when user clicks on the URL, Pulse Desktop Client gets invoked and connects to the VPN.
• Pulse SAM IPv6 Support	• Pulse Desktop Client now supports IPv6 traffic tunneling in Pulse SAM mode on Windows 10, Windows 8.1 and Windows 7 platforms.
• Automatic Keyboard popup on Surface Pro PSAM + L3 Tunnel Co-existence	• When the users select the username or the password field on Pulse Desktop Client installed on a Windows Surface device, the virtual keyboard automatically pops up so that user can enter the credentials.

Learn More

Resources

- Pulse Connect Secure datasheet
- Pulse Policy Secure datasheet
- Pulse Cloud Secure product brief

www.pulsesecure.net

About Pulse Secure, LLC

Pulse Secure, LLC is a leading provider of access and mobile security solutions to both enterprises and service providers. Enterprises from every vertical and of all sizes utilize Pulse Secure's Virtual Private Network (VPN), Network Access Control (NAC) and mobile security products to enable secure end-user mobility in their organizations. Pulse Secure's mission is to provide integrated enterprise system solutions that empower business productivity through seamless mobility.

Corporate and Sales Headquarters
Pulse Secure LLC
2700 Zanker Rd. Suite 200
San Jose, CA 95134
www.pulsesecure.net

Copyright 2019 Pulse Secure, LLC. All rights reserved. Pulse Secure and the Pulse Secure logo are registered trademarks or Pulse Secure, LLC. All trademarks, service marks, registered marks, or registered service marks are the property of their respective owners. Pulse Secure assumes no responsibility for any inaccuracies in this document. Pulse Secure reserves the right to change, modify, transfer, or otherwise revise this publication without notice.