PRODUCT BULLETIN

PULSE CONNECT SECURE, PULSE POLICY SECURE AND PULSE CLIENT UPDATES FOR 9.1R3

Bulletin Date

October 2019

Applicable to All

Regions Effective

Change Date

October 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 9.1R3 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 customer requirements, Cisco ACS migration use cases, support for SDP enabled client on macOS and FQDN based Split tunneling improvements.

What's New

Common Features for Pulse Connect Secure and Pulse Policy Secure

Key Feature	Benefit
Consolidated system and troubleshooting logs	The various system logs and troubleshooting logs that help in investigating user access issues and system issues can be configured and accessed using the Log Selection page.
Connect to nearest available Domain Controller	The LDAP authentication configuration is enhanced in 9.1R3 to locate the nearest Microsoft domain controllers, which are spread across the globe, by resolving DNS SRV records.
Zero touch provisioning	From 9.1R3 release, PCS can detect and assign DHCP networking settings automatically at the PCS VM boot up. In the script included in the PSA-V package, the PCS parameters should be set to null in order to fetch the networking configuration automatically from the DHCP server. Note: This feature is not supported on PSA hardware.
VMware tools support	From 9.1R3, VMware support is qualified for VMware 10.3.10, ESXi 6.7 Update 2c.
Debug Log storage expansion	From 9.1R3 release, the maximum debug log size is increased to 1024 MB on hardware platforms.
Periodic iostat data collection	From 9.1R3 release, the "iostat" information is gathered periodically and made available as part of node monitoring in system snapshot.

Pulse Connect Secure 9.1R3

From 9.1R3 release onwards, Pulse Secure is introducing mTLS support for Pulse Secure Software Defined Perimeter. 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 Connect Secure 9.1R3.

Highlighted Features in this Release

Key Feature	Benefit
PCS hosted in OpenStack cloud	OpenStack is an open source cloud computing platform that allows deploying and managing a cloud infrastructure as an IaaS service. As part of this release, Pulse Secure supports deploying PCS KVM in OpenStack cloud.
Control copy/paste option for a user from an HTML5 session	9.1R3 release provides option to the administrators as well as end-user to enable/disable copy/paste from HTML5 RDP sessions. This option will be available under User Roles as well as Admin Created Bookmarks".
Restricting access to default resource policies	From 9.1R3 release, for a fresh installation, the following predefined resource policies are set to "Deny" state by default. ▪ Web Access Resource Policy "Initial Policy for Local Resources" ▪ Windows File Access Resource Policy "Initial File Browsing Policy" Also, the default policy for VPN Tunneling is not provided.
IKEv2 Fragmentation	IKEv2 packets can be larger than the MTU especially the IKE_AUTH packets which include the certificate chain. These larger IKE packets get fragmented in the intermediate devices. This feature implements fragmentation at IKE level and avoids IP fragmentation.
MSS value for TCP connections on Tun devices	Due to larger IPv6 header as compared to IPv4, if the MSS of the PCS external interface is not set appropriately, the packets would be dropped on the external interface. This feature enables to set MSS to a lower value so that TCP connections are not dropped for 6-in-4 cases or when there is NAT translation somewhere in the network before reaching PCS.
Enhancements to Local Authentication Server default password	From 9.1R3 release, for a fresh installation, the valid password range defined is 0-999. Minimum length 10 and maximum length 128 are set as default values.

Pulse Cloud Secure 9.1R3

In 9.1R3 release, no new features included in the product.

Pulse Policy Secure and Profiler 9.1R3

Highlighted Features in this Release

VSYS support in PAN Firewall	PPS can provision user's authentication details and Resource/IOT policies to specific VSYS in PAN firewall.
MYSQL support in PPS	MYSQL authentication server is added as vendors in SQL vendor list.
Local user account import through CSV	Import user accounts via CSV file in System local auth server. The local authentication server is an authentication database that is built in to PPS.
SNMP Enforcement	SNMP VLAN enforcement support is now expanded for 3Com, Juniper and Dell switches. SNMP ACL enforcement support is now expanded to support 3Com and Dell switches (Juniper support already exists).
One-to-one NAT support	With this feature, a configurable option is provided to admin in "Infranet Enforcer Auth Table Mapping Policy" page, which allows the entry for end user behind 1-to-1 NAT to be provisioned on firewall. Prior to this feature when One-to-One NAT deployment is detected by PPS, end user is labelled as being behind NAT and its entry is not pushed to the firewall.
SIEM integration	PPS supports integration with IBM Qradar and Splunk. The overall solution provides end-to-end security. The SIEMs can send this alert information to PPS and then PPS can leverage its existing functionality of admission control, L2/L3 enforcement and provide role-based access control to secure the network.
FortiGate Firewall direct integration	With this feature PPS can now directly enforce on FortiGate firewall without the need for having an additional FortiAuthenticator.
vTM and PPS Integration for Load Balancing	This feature helps achieve a more even distribution of sessions across PPS instances using vTM load balancer. vTM can now use additional three parameters for better load balancing.

Pulse Secure Desktop Client 9.1R3

From 9.1R3 release onwards, Pulse Secure is introducing mTLS support for Pulse Secure Software Defined Perimeter.
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 9.1R3.

Highlighted Features in this Release

Key Feature	Benefit
EKU/OID filtering for client certificate selection	Pulse Desktop Client will now provide the administrator an option to specify EKU Text or EKU OID for filtering the certificates displayed in the certificate selection prompt during Cert-Auth. It will filter the certificates automatically, so that only relevant certificates are displayed.
Optional loading for KEXT Component	Pulse Desktop Client on macOS will now load KEXT component only if "Traffic Enforcement" or "Lockdown mode" options are enabled. Otherwise, KEXT component which requires high privilege access is not loaded.
Pulselauncher.exe to access certs from System Store	Pulse launcher tool (pulselauncher.exe), which is a is standalone client-side command-line program, can now access certificates located in system store allowing for certificate-based authentication from the tool.

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