



Pulse Policy Secure

Complete endpoint visibility and Zero Trust Network Access Control



Highlights

- Centralized visibility and policy management of all endpoints, including IoT
- Granular assessment of endpoint security posture before allowing access
- Dynamic network segmentation based on user role and/or device class
- Seamless roaming between remote and local, using Pulse Connect Secure Integration
- Granular integration with Pulse vADC for a scalable, resilient and responsive solution
- BYOD onboarding integration with Pulse Workspace MDM or 3rd party EMM
- REST API integration with security ecosystem
- Scales for organizations of any size

Benefits

- End-to-end Zero Trust Network Access security
- Reduced threat response time
- Reduced risk from lateral spread of threats
- Automated policy enforcement, reduced auditing burden
- Simple and fast deployment

Product Description

Modern networks experience a proliferation of connected endpoints; BYOD connectivity is now surpassed by IoT. Every additional endpoint increases the risk to be compromised and give attackers an opportunity to gain further access into the network and to corporate resources. To limit this risk, an endpoint's security posture must always show current software security updates, virus definitions, and so on. Also, users must only be given the least amount of access necessary to perform their role.

Pulse Policy Secure (PPS) provides complete visibility and Network Access Control (NAC) for all endpoints, regardless of their network location. Its open, high-performance design helps small and large organizations to easily enforce endpoint security compliance and Zero Trust security.

Pulse Policy Secure continuously enforces foundational security policies and controls network access for managed, unmanaged, and IoT endpoints. PPS uses Zero Trust principles to manage network access by validating the user, a device's security posture and connects the device with least privilege access policy.

The open platform integrates with a wide range of switching, Wi-Fi and NGFW solutions to enforce access policies. Bidirectional integration with 3rd party security solutions improves overall security efficacy with automated endpoint access enforcement. Automated responses to Indicators of Compromise (IoC) reduces remediation time and streamlines administrative resources. PPS integrates with a wide range of NGFWs such as Palo Alto Networks, Checkpoint, Juniper and Fortinet, as well as SIEM solutions such as IBM Qradar and Splunk.

Key Components

The Pulse Policy Secure solution includes three components:

- **Pulse Profiler** identifies and classifies endpoint devices, including IoT. It provides end-to-end visibility, reporting and behavior analytics.
- **Pulse Policy Secure** provides a high-performance policy engine that leverages contextual information from users, endpoints, and applications. With a unified, open framework and policy engine, administrators can apply granular rules for dynamic monitoring, reporting, and access control of all endpoints, anywhere on the network, to minimize access risks.
- **Pulse Client** offers agent and agentless options for pre- and post-admission control. The solution incorporates the Host Checker functionality, which verifies an endpoint's security posture. This is the same Pulse Client used for our Pulse Connect Secure VPN solution and runs on Windows, Mac, Linux, Android and IOS platforms.

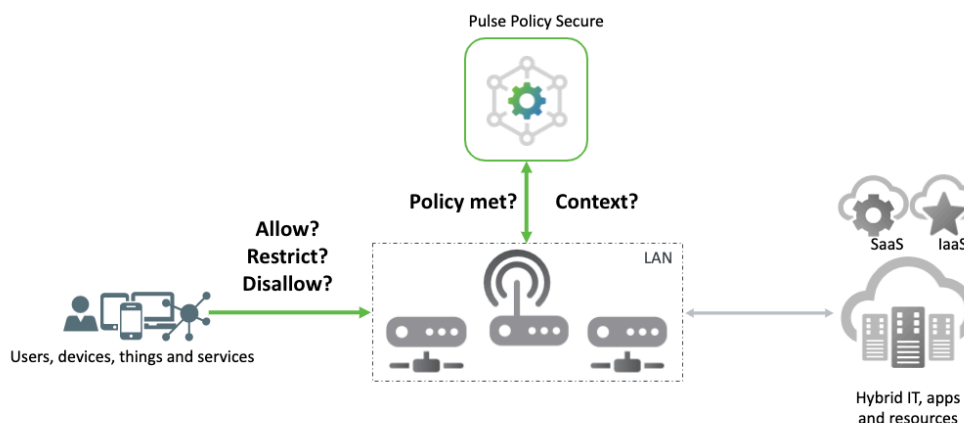


Figure 1: Access Decisions for endpoints

Use Case Overview

Pulse Policy Secure helps to adapt Zero Trust Network Access security for small and large organizations. Enterprises use PPS to enforce endpoint policy compliance for employees, guests, and contractors regardless of location, device type, or device ownership. Users enjoy greater productivity and the freedom to work anywhere without limiting access to authorized network resources and applications. BYOD onboarding optimizes the user experience by allowing workers to use their preferred device. Pulse Policy Secure gives you complete visibility of managed and unmanaged network devices.

Visibility

To protect your network endpoints, you need to see what endpoints are connected. Complete visibility enables the required insight to dynamically identify and classify all managed and unmanaged endpoints.

CHALLENGES	PULSE POLICY SECURE SOLUTION
Profiling	Pulse Profiler dynamically identifies and enables automatic and custom classification of both managed and unmanaged endpoint devices, to provide operational visibility, reporting and policy-based controlled access to networks and resources based on the user, device, applications and other attributes.
Behavioral Analytics	Pulse Profiler continuously performs behavioral analytics and builds baseline behavior profiles for IoT devices by collecting and correlating NetFlow, user, and device data. This is used to detect anomalous device activity, anomalous user access, domain generation attacks and MAC spoofing.
Numerous Device Types	Pulse Profiler can automatically classify devices against a growing database of over 2.3M unique fingerprints. The solution profiles endpoints static or dynamic IP addresses and actively scans open ports to detect MAC spoofing.

The Internet of Things (IoT)

Enterprises today merge IoT devices with the IT environment to improve business. Pulse Policy Secure offers enterprises the ability to discover and secure these devices.

CHALLENGES	PULSE POLICY SECURE SOLUTION
Discovery, profiling and segmentation of IoT devices	Pulse Profiler discovers managed and unmanaged IoT devices. It profiles them so they can be matched to specific access policies. Dynamic segmentation limits the risk of threats spreading laterally and helps with regulatory compliance in healthcare for example.

Device Onboarding and Policy Compliance

Pulse Policy Secure prevents unauthorized network, application, or data access by dynamically assessing and remediating device security before the device connects to the enterprise for both VPN and Wi-Fi access. This protects the corporate network from infected devices and enforces consistent, cross-network access policies. It also ensures only authorized workers have access to enterprise resources based on their role, location, and time of day.

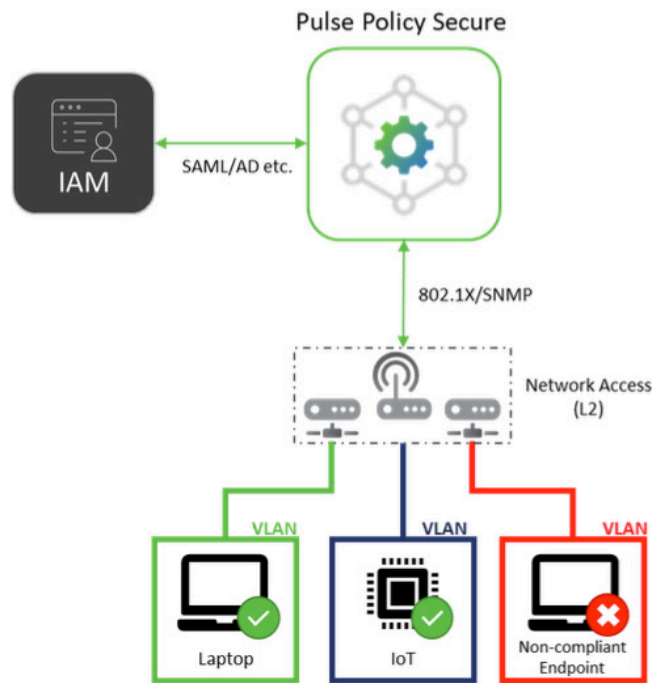


Figure 2: Dynamic access control and network segmentation (L2)

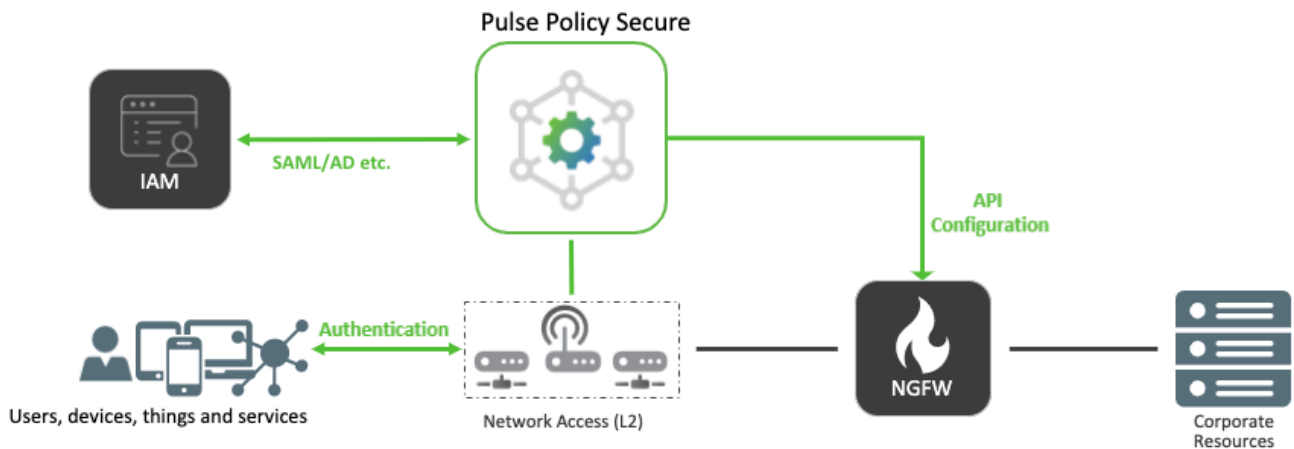


Figure 3: Dynamic access control at perimeter (L3)

CHALLENGES	PULSE POLICY SECURE SOLUTION
Guest User Support	Pulse Policy Secure provides a self-service portal with a customizable interface. It is a highly scalable enterprise guest access platform that supports thousands of guest users. For additional control, secure guest access can be enabled by an admin such as a receptionist, or by a sponsor whom approves the guest's access request. PPS integrates with wireless controllers such as Aruba, Cisco, Huawei, Juniper Mist, Meraki and Ruckus.
BYOD Onboarding	Pulse Policy Secure empowers employees to use their personal devices for work with self-service onboarding of personal laptops and mobile devices.

KEY FEATURES	
Pulse Profiler	Identifies and classifies endpoint devices, including IoT. It provides end-to-end visibility, reporting and behavior analytics.
RADIUS/802.1X support	An integrated, high performance RADIUS authenticates users and devices that are forwarded from industry-standard 802.1X functions on network switches and wireless controllers.
TACACS+ support	Use the TACACS+ authentication system to distribute policies to the access infrastructure. Supports Two-Factor Authentication with Smart Cards.
Host Checker	Identifies the security posture of the device. Options include: OS or software patch status, active apps.
Session federation	Active VPN sessions seamlessly migrate to the local network without the need to re-authenticate.
UEBA Analytics	Correlation of user access, device data, and system logs in a new analytics engine integrates with Pulse One management solution.
Identity-based admission control	Shares identity context with NGFWs from vendors such as Fortinet, Palo Alto Networks, Checkpoint, and Juniper SRX, enabling each to be employed as policy enforcement points on the network perimeter.
Automated Threat Response	Leverages external threat intelligence alerts from NGFW or SIEM solutions to take automated actions at the device connection level. PPS' policy engine leverages rich contextual information to allow various mitigating actions based on threat severity.
Captive portal	Provides user-friendly access control for guests and contractors.
Self-service Guest access support	Provides secure, simple and differentiated guest access.
Wizard-based configuration	Simplifies configuration tasks for administrators to avoid mistakes and faster deployment.
Granular auditing and logging	Granular logging capabilities of system, user and device events in a clear, easy to understand format. Can be analyzed locally or shared with external syslog solutions or SIEMs such as IBM Qradar and Splunk. Supports WELF format and WELF-SRC-2.0-Access Report.
Centralized policy management	Saves administrative time and cost and a superior user experience by delivering common remote and local access control policy implementation and enforcement across a distributed enterprise.
REST API	Standardized interface for third party systems such as NGFWs and SIEMs to integrate with Pulse Policy Secure and limit an endpoint's access on the local network.
Flexible deployment options	Pulse Policy Secure runs on physical, virtual and cloud platforms. See the Supported Platforms Guide for details.



**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.

Copyright 2020 Pulse Secure, LLC. All rights reserved. Pulse Secure, Pulse Secure Logo, and Pulse SDP are registered trademarks of 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.



[linkedin.com/company/pulse-secure](https://www.linkedin.com/company/pulse-secure)



twitter.com/PulseSecure



www.facebook.com/pulsesecure1



info@pulsesecure.net