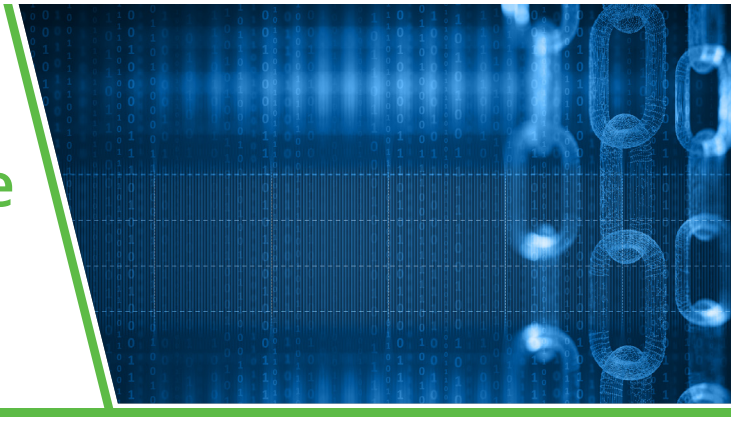
Pulse Secure®

Integrated Threat Defense with Pulse Policy Secure

Zero Trust Network Access Control
Throughout the Connectivity Lifecycle



Overview

To protect data and resources, enterprise security personnel use solutions such as Next-Generation Firewalls (NGFWs) to control access to resources and monitor traffic flows, and Security Information and Event Managers (SIEMs) to analyze and cross-correlate events. However, these individual solutions' actions are limited to sending alerts, or enforcing policies on the traffic that passes through them. Network Access Control (NAC) solutions have traditionally enforced an endpoint's security posture, before connecting to the network. Bidirectional integration with the security ecosystem enables a NAC to increase overall security efficacy by taking remedial action on an endpoint's connectivity, after receiving alerts from other security solutions. Automated security enforcement with a NAC provides benefits such as:

- Reduced threat response time
- Streamlined security operations
- Limited lateral spread of threats
- Automated security compliance, easier audits
- More granular policies with contextual information

Pulse Policy Secure (PPS) integrates with network and security infrastructure devices such as switches, wireless controllers and next-generation firewalls (NGFW), but also with solutions such as identity and access management (IAM), SIEM, Advanced Threat Protection (ATP) and Enterprise Mobility Management (EMM). PPS enables automated, actionable access decisions based on contextual data such as identity, security posture and location. Based on a Zero Trust access framework, Pulse Policy Secure continuously enforces the trust level of an endpoint during its connectivity lifecycle and quarantines it when a behavioral anomaly is detected.

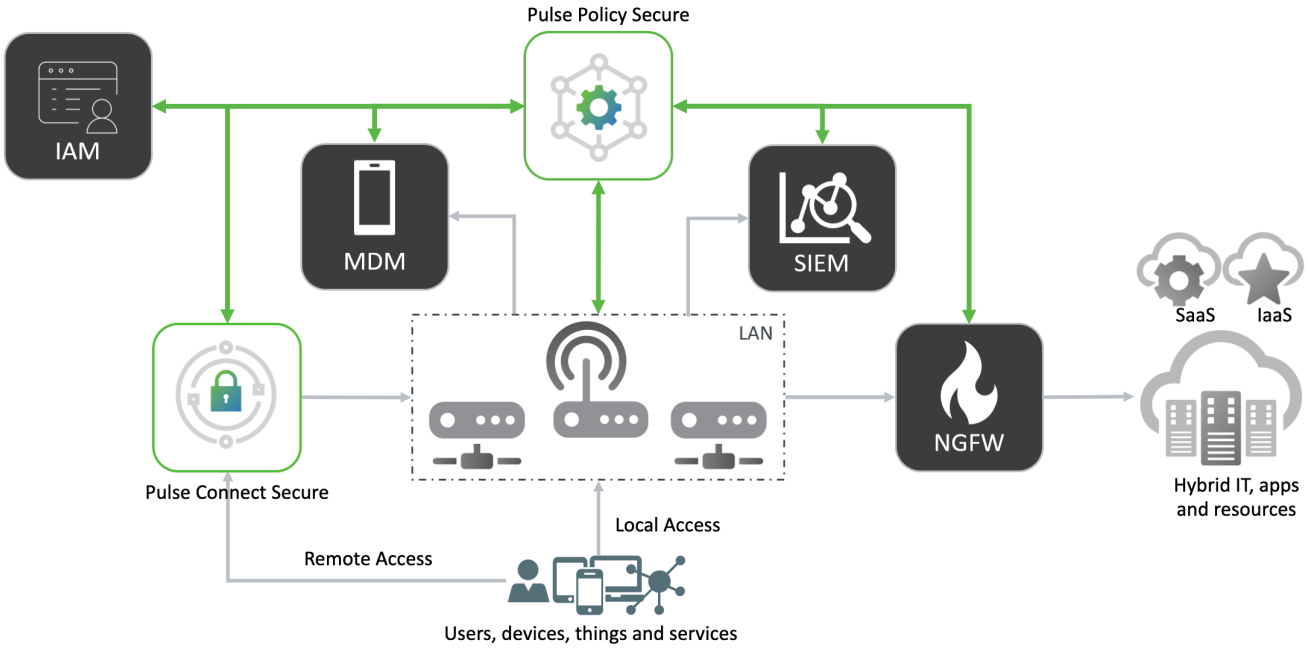


Figure 1: PPS integrations into network and security ecosystem

Integrations for Continuous Trust Assessment

Network Access

The best showcase of the Zero Trust principle "Never Trust, Always Verify" is when a user wants to connect to the network. Pulse Policy Secure first validates the user and the device against the policy. Then, PPS connects the device with the access infrastructure in line with that user's role. This dynamic network segmentation limits the lateral spread of threats between different classes of (IoT) devices and users. PPS integrates with leading switching and WiFi solutions from vendors such as Cisco, Juniper, Aruba and Ruckus using the common 802.1X standard, or SNMP. Dynamic network perimeter provisioning provides another layer of access control. NGFW policies can leverage additional contextual information such as the user's identity or location. PPS integrates with NGFW solutions such as Palo Alto Networks, Checkpoint, Juniper and Fortinet, to provide this contextual information about the endpoint.

Endpoint Compliance

Endpoints use a wide variety of software; the Operating System, security utilities such as Anti-Virus, as well as user-level apps. All this software receives periodic updates for feature enhancements and security fixes. The Host Checker feature continuously assesses the security posture of the device by validating the software update history and active apps. Once PPS grants network access to a user and/or device, it continuously monitors the security posture throughout the connectivity lifecycle. If the security posture changes, for example because the user launches a shadow IT app that violates the policy, PPS immediately moves the endpoint into a restricted network environment.

PPS helps organizations to minimize risk by automatically enforcing endpoint compliance. The Host Checker can interact with Windows Management Instrumentation, Windows Defender, Microsoft Security Essentials, or the Pulse Connect Secure VPN client for even more granularity.

Identity and Access Management (IAM)

The authentication mechanism validates a user's identity and defines its role. The authentication system can leverage contextual information, based on time, geolocation or behavior. For example, if authenticated sessions already exist in a different geolocation, the user can be subjected to additional authentication methods such as two-factor authentication (2FA). Pulse Policy Secure integrates with IAM solutions using protocols such as SAML (Ping, Okta, Duo etc.), Active Directory (Microsoft), or even RADIUS/TACACS+ or LDAP for more isolated environments. PPS comes with a built-in RADIUS service.

Security Events

A solid, layered security strategy requires the continuous analytics of network flows and events, using solutions such as Next-Generation Firewalls (NGFWs), Security Information and Event Management (SIEM), or Advanced Threat Detection (ATD). Bidirectional integration with Pulse Policy Secure improves overall security efficacy, with actionable, automated responses enforced at the network access level. Automated responses to Indicators of Compromise (IoC) reduces remediation time and streamlines administrative resources.

PPS integrates with leading NGFWs, such as Palo Alto Networks, Checkpoint, Juniper and Fortinet, as well as SIEM solutions such as IBM QRadar and Splunk.

Use case: NGFW Alert

When a NGFW discovers a threat, it alerts Pulse Policy Secure, using standard syslog. Pulse Policy Secure can quarantine the suspect device to a restricted access environment to remediate the problem and prevent lateral spread of the threat.

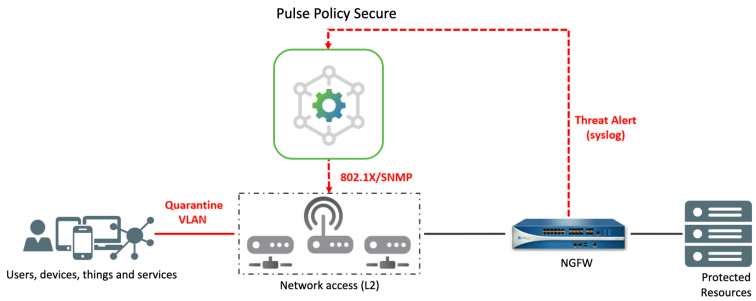


Figure 2: Real-time response to NGFW alert

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.

linkedin.com/company/pulse-secure
www.facebook.com/pulsesecure1
twitter.com/PulseSecure
info@pulsesecure.net