Pulse Policy Secure

Product Overview

As part of the Secure Access Solution from Pulse Secure, Pulse Policy Secure is a mobile-ready NAC solution that offers extensive visibility on the network activity for security and performance. After seeing what is on the network, you now have a centralized granular policy platform that integrates with market leading network vendors for enforcement. Addressing numerous industry compliance requirements from government to healthcare-finance, Policy Secure streamlines everyday mobile access challenges like BYOD and guest-access, while creating network traffic flows clean of malware infections and many other risks associated with security breaches.

Product Description

Pulse Policy Secure delivers an easy-to-use BYOD ready granular access control and visibility solution that is context aware for the most complex datacenter and cloud environments. Pulse Policy Secure enables safe, protected network and cloud access for a diverse user audience over a wide range of devices. The Pulse Policy Secure provides best-in-class performance and scalability while delivering centralized policy management with visibility, access control, and simplifying deployment, administration, and management.

Pulse Policy Secure provides visibility into the network by detecting and continuously monitoring the network. It provides visibility for on-site and remote endpoints/users connecting through VPN. Pulse Policy Secure can be enabled at Layer 2 leveraging 802.1X/RADIUS; at Layer 3 using an overlay deployment; or in a mixed mode using 802.1X for network admission control and a Layer 3 overlay deployment for resource access control. It fully integrates with any vendor's 802.1X/RADIUS;-enabled wireless access points, such as Cisco, HP/Aruba Wireless, Brocade/ Ruckus Wireless, or any vendor's 802.1X-enabled switches, such as Juniper Networks EX Series Ethernet Switches, which, when deployed with Pulse Policy Secure, deliver additional, rich policy enforcement capabilities. Existing 802.1X infrastructure may be leveraged, as well as any Juniper, Palo Alto Networks firewall or Fortinet firewall, for policy enforcement and granular access control. Pulse Policy Secure also supports the Juniper Networks SRX Series branch firewalls, allowing them to configure Pulse Policy Secure as a RADIUS server, saving cost while addressing 802.1X support for branch offices.

Pulse Policy Secure also added support for device visibility and policy enforcement on switches using SNMP (Simple Network Management Protocol) as an alternative to 802.1X. Pulse Policy Secure uses SNMP v1/v2c/v3 to discover L2/L3 switches and discover endpoints via SNMP Traps (LinkUp, LinkDown, MAC notification, and Port security). SNMP-based policy enforcement can be applied to endpoints running the Pulse Client, and to clientless endpoints where the MAC address is discovered via SNMP. For endpoints running the Pulse Client, role assignment may be based on compliance; for clientless endpoints, role assignment is based on MAC address.

Pulse Policy with SNMP simplifies NAC deployment without using 802.1x supplicant and leverage existing network device infrastructure that may not support 802.1X feature. With SNMP enforcement, NAC is easy to deploy and achieve comprehensive compliance and role-base access.

[1]Formerly known as Pulse Secure Unified Access Control

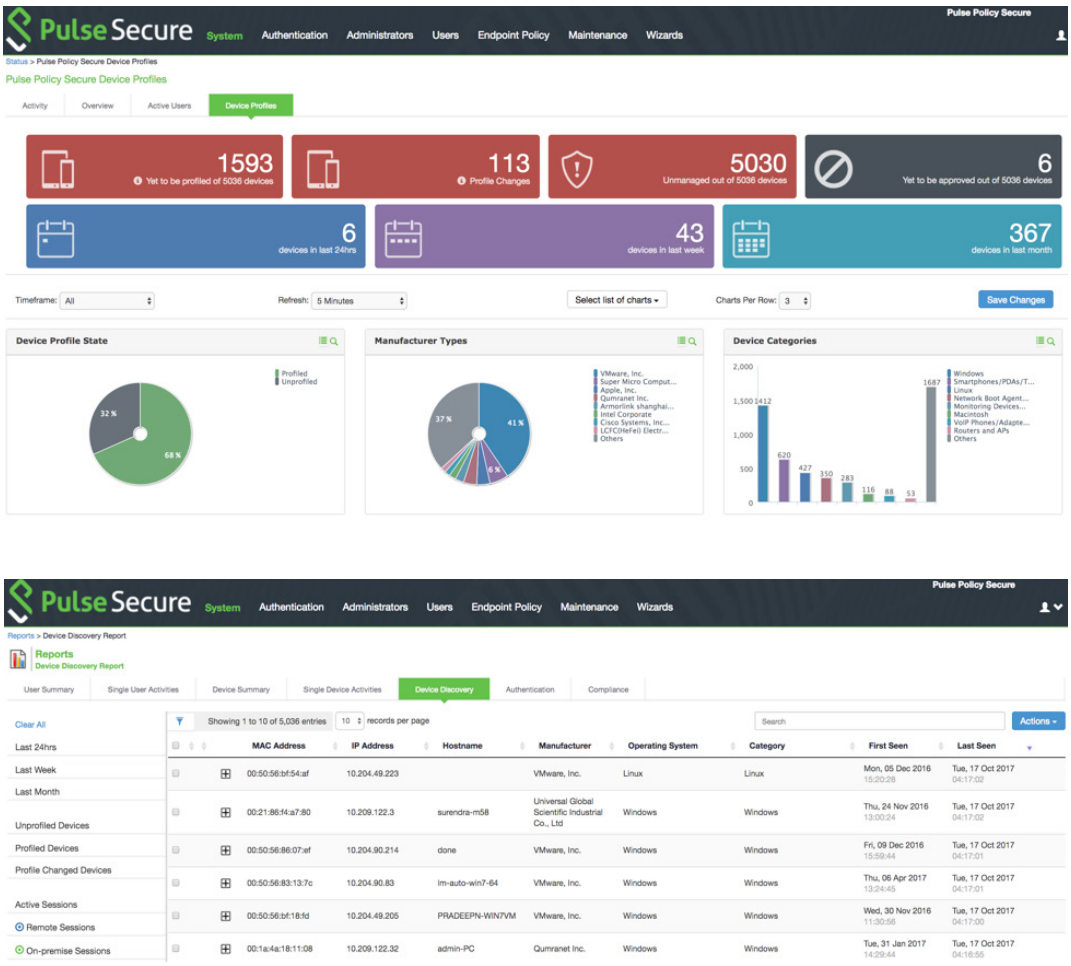

Image 1 - Pulse Policy Secure Management Console

Visibility with Pulse Secure Profiler

Pulse Policy Secure offers an on-box profiler solution (reference Image 1) that dynamically identifies and classifies devices that are using client and clientless software. It enables access control to resources based on the type of the device. It uses different fingerprinting methods to classify devices with DHCP Fingerprinting (Helper Address or RSPAN port), SNMP/SNMP Traps, CDP/LLDP, HTTP User Agent, Nmap, WMI and MDM. Our intuitive dashboard offers a single pane of glass view for all devices on the network. Additional contextual information is available for troubleshooting and visibility purpose. Pulse Secure Profiler continuously monitors devices and re-evaluates classification based on on-going changes. Pulse Secure Profiler classifies endpoints coming from VPN or On-premise connection, so that administrators can get a complete visibility into their network. Pulse Secure offers a standalone profiler solution. It supports Active/Active cluster and non-cluster multiple Pulse Policy Secure or Pulse Connect Secure deployments within the data center.

Network Security and Application Access Control Integration

Pulse Policy Secure leverages additional network components to ensure secure context aware network and application access control, address specific use cases, and centralize network policy management. It integrates with the intrusion prevention system (IPS) capabilities of the SRX Series gateways for both data center and branch, as well as the standalone Juniper Networks IDP Series Intrusion Detection and Prevention Appliances, to deliver broad application traffic visibility—mitigating insider threats by isolating them to the user or device level, and employing an applicable policy action against an offending user or device. Pulse Policy Secure ties user identity and role information to network and application access, addressing regulatory compliance and audit demands. When deployed with the Juniper SRX Series, Palo Alto Networks and Fortinet firewalls, Pulse Policy Secure provides the ability to provision user session information to an application-aware firewall based on the role of an authenticated user. This empowers customers, with next-generation firewalls, to utilize the user's role information for the application of granular application-access policies based on

[2]Only for SRX Series gateways running Junos OS 12.1 or higher

a specific user's identity. Pulse Policy Secure also supports Layer 2 through Layer 7 policy enforcement with Juniper SRX Series Firewalls, offering unparalleled visibility into application traffic at Layer 7 by leveraging SRX Series Firewalls for the data center.

Pulse Policy Secure also enables any user authenticated via Microsoft Active Directory to be silently provisioned to SRX Series gateways, transparent to the end user. End users do not need to launch a Web browser and authenticate via captive portal. Pulse Policy Secure enables dynamic, identity focused, role-based firewalling with SRX Series gateways, without any user interaction required.

Likewise, when deployed with Palo Alto Networks or Fortinet Firewalls, Pulse Policy Secure auto-provisions User Identity, IP address and role information so that access policies can be enforced. Via the host-checking capabilities of the Pulse Client or a MDM Client, Pulse Policy Secure detects unauthorized devices for remediation and compliance enforcement.

To aid in Bring Your Own Device (BYOD) initiatives, Pulse Policy Secure works with market leading Mobile Device Management (MDM) systems to extend its context aware capabilities, deployment simplicity and management cooperation. Integration between these systems enables IT professionals to create policy based on mobile device type, state, location, installed applications, etc. Policy reporting integrates this information within the management console simplifying security management operations.

Federation

Pulse Policy Secure enables the federation—or sharing— of user session data with Pulse Connect Secure (SSL VPN), seamlessly transitioning remote access user sessions to LAN user sessions at login, or alternatively local LAN user sessions into remote access sessions. The federation of LAN access and remote access session data is a vital part of the context awareness and session migration capabilities of Pulse Secure. This enables a remote access user connected via SSL VPN to Pulse Policy Secure to be granted seamless access to the LAN through the same or different Pulse Policy Secure instances, without re-authentication. No re-authentication is required, enabling "follow-me" policies regardless of the user's device or worldwide location.

Guest Access Management

Pulse Policy Secure offers built-in, advanced guest user access control capabilities to deliver a simple, seamless, and authorized network resource access for customers, partners, and contractors. Guests can self-register to request and obtain appropriate authorized access from any device. After registering, guests can be automatically notified of their authorized and time-limited guest credentials via SMS or email. This solution allows our customers to automatically manage network use by guest and contractors, and reduces threats from unauthorized users and compromised devices. Pulse Policy Secure also offers sponsored-based guest access, where guest registration request goes to sponsorer and they can approve/deny guest request without involving IT team.

Additional enterprise-grade features are: Customization with corporate branded guest access portal, an option to create unique data-entry fields for guest names, sponsors, email, mobile numbers and acceptance of use. It also enables selected guest user enterprise account managers to provision temporary guest access accounts for corporate guest users, to create bulk accounts for numerous guest users, and to send automatically guest user credentials via email or text message to an expected guest user, simplifying the network guest access process.

Endpoint Compliance and Patch Assessment

Pulse Policy Secure offers an industry-leading variety of endpoint host checks to ensure compliance, including predefined checks for third-party endpoint security software including anti-virus, firewall, anti-malware/anti-spyware applications, and custom rules for a variety of other endpoint requirements. Pulse Policy Secure offers device patch assessment checks, including endpoint inspection for targeted operating system or application hot fixes, with optional integration for Windows for devices that do not meet policy and require patch updates.

Open Standards

Pulse Secure is a strong supporter of open standards, including those of the Trusted Computing Group's (TCG) Trusted Network Connect (TNC) Work Group, which ensure interoperability with a host of network and security offerings. Through its support of the TNC standard Statement of Health (SOH) protocol, Pulse Policy Secure with optional SOH license interoperates with the Microsoft Windows SOH and embedded Microsoft Network Access Protection (NAP) Agents, enabling you to use existing Microsoft Windows 10, Windows 8.1, Windows 8, Windows 7, Windows RT, and/or Windows Vista. Pulse Policy Secure also supports the TNC's open standard Interface for Metadata Access Point (IF-MAP) through a license option, enabling integration with third-party network and security devices—including nearly any device that supports the IF-MAP standard and collects information about the happenings on, or status of, your network. The Pulse Policy Secure can leverage this data when formulating access control decisions, taking any necessary and appropriate actions.

Quick, Easy Deployment

Network access control with Pulse Policy Secure is deployed quickly and easily. It includes an optional "step-by-step" configuration wizard to aid administrators in configuring common network access control (NAC) deployment scenarios. Pulse Policy Secure also allows you and your users to ease into policy enforcement by enabling access control to be phased in, as well as allowing it to be run in audit mode. Light-touch deployment wizards are available to support best practices guidelines. Also, Juniper SRX Series gateways can be deployed in transparent mode with Pulse Policy Secure, simply acting as a "bump in the wire" (BITW), eliminating the need to modify your network's routing topology. Mobile Device Management (MDM) systems such as those from MobileIron, Airwatch, and Microsoft

Intune can be leveraged to transparently deploy and configure Pulse Secure clients to Android and iOS devices facilitating deployment efforts to remote devices. And lastly, it has also been tested to work with select Cisco and HP Aruba Network Wireless LAN equipment.

Architecture and Key Components

Pulse Policy Secure uses three core components to deliver a context (who, what, where, when, etc) aware network and application access control:

PSA Series Appliance Family (PSA Series Hardware and PSA-V Series Virtual)

Pulse Policy Secure is the network and application access control software which runs on the Pulse PSA Series Appliance Family (PSA Series Hardware and PSA-V Series Virtual - virtual machine over KVM or VMWare hypervisors). Pulse PSA Series Hardware are purpose-built, centralized policy management hardware that work with the Pulse Secure Client or in clientless mode to obtain user authentication, device security posture, and device location data from a user's endpoint device.

This data creates dynamic policies that are propagated to policy enforcement points throughout the distributed network worldwide.

Pulse Policy Secure leverages the policy control engine from Pulse Connect Secure, as well as their ability to seamlessly integrate with existing authorization, authentication,and accounting (AAA) and identity and access management (IAM) infrastructure. It also integrates RADIUS capabilities and enhanced services from Pulse Secure's SBR (Steel-Belted Radius) Enterprise Series Servers, to support an 802.1X transaction when a mobile or non-mobile device attempts network connection. Pulse Policy Secure and Pulse Series Appliance Family (PSA Series Hardware and PSA-V Series Virtual) may also be licensed as standalone RADIUS servers.

You may simply deploy any Pulse PSA Series Appliance Family (PSA Series Hardware and PSA-V Series Virtual) running Pulse Policy Secure with your existing vendor-agnostic 802.1X switches or wireless access points.

Pulse Secure Client and Clientless Mode Deployments

Pulse Secure Client is our integrated, multifunction enabling interface, which can be dynamically downloaded and provisioned to endpoint devices in real time. It provides the user interface to Pulse Policy Secure, as well as other Pulse Secure services. The same Pulse Secure client can be used in wired, wireless, or combined deployments. Pulse Policy Secure also provides a clientless mode for circumstances where software downloads are not feasible. Pulse Policy Secure can be delivered based on role, linking client-based or clientless access dynamically to user or device identity.

Pulse Client or clientless mode collects user and device credentials, and assesses the device's security state. It leverages and integrates with the native 802.1X supplicant available within Microsoft Windows to deliver comprehensive L2 access control. Pulse Client can also support native 802.1X supplicants on Apple Mac OS X and iOS, and Google Android devices for L2 authentication. Pulse Client, along with Pulse Policy Secure, also provides L3 authentication and IPsec tunneling with any Juniper firewall, including the SRX Series, as an optional secure transport to enable encryption from the endpoint to a firewall for session integrity and privacy, as well as single sign-on (SSO) to Microsoft Active Directory and silent provisioning to SRX Series gateways.

Pulse client includes our Host Checker functionality, enabling you to define policy that scans both mobile and non-mobile devices attempting to connect to your network for a variety of security applications and states both through the Pulse client and leveraging attributes from Mobile Device Management (MDM) systems from AirWatch, MobileIron , Microsoft Intune, and others. For Windows and Mac OS X based devices, Host Checker scans for active antivirus, anti-malware, and personal firewalls. It also enables custom checks of elements such as registry and port status for Windows-based devices, and can perform a Message Digest 5 (MD5) checksum to verify application validity. Mobile devices running Apple iOS or Android initially connect to a Pulse Connect Secure (SSL VPN) which runs Host Checker on the mobile device to check its security posture. This host check includes device and OS identification, detection of jail broken or rooted devices, device type, and more. It can also leverage integration with MDM systems to execute health check and set policy based on a wider set of attributes for Apple iOS and Android-based devices. If the mobile device passes the host check and the user is authenticated, appropriate network access is granted. At that time, the user's session information is shared between Pulse Connect Secure and the Pulse Policy Secure via the TNC IF-MAP protocol. Pulse Secure then pushes the appropriate access policies for the user and mobile device to the Juniper SRX, Palo Alto Networks or Fortinet firewall.

Pulse Policy Secure and Host Checker can also assess a Windows endpoint during machine authentication, mapping the device to a different role and placing it into remediation based on assessment results. This deployment is simplified through predefined Host Checker policies, as well as the automatic monitoring of antivirus and antispyware signatures and patches for the latest definition files for posture assessment. Network access is also directly tied to the presence or absence of specific, defined operating systems, application patches, and "hot fixes." Role-based, predefined patch management checks are conducted according to the severity level of the vulnerability.

Pulse Client also integrates with antispyware/anti-malware protection for Microsoft Windows endpoint devices that attempt network access, scanning device memory, registry and load points, and preauthentication for spyware and keyloggers.

It supports Layer 2 and Layer 3 authentication and device integrity assessments for devices running Microsoft Windows 10 Enterprise (64-bit), Windows 8.1 / 8 Enterprise (32- and 64-bit), Windows 7 Enterprise (230 and 64-bit), Windows Vista (32- and 64-bit) operating systems. It also supports Layer 3 authentication and device integrity assessments for devices running Apple Mac OS X 10.6 (or higher) operating system software, and devices running Apple iOS or Google Android (integration with Pulse Connect Secure only).

[2]Running Junos OS 12.2 or higher

[4]Only for SRX Series gateways running Junos OS 12.1 or higher

Policy Enforcement Points (PEPs)

Pulse Policy Secure enforcement points include any 802.1X compatible wireless access point or switch, virtual and physical This includes the Juniper Networks EX2200, EX3200, and EX4200 Ethernet Switches, as well as the EX8200 line of Ethernet switches. It also includes the WLA Series and AX411 WLAN access points; any Juniper firewall platform, including the SRX Series gateways; J Series Services Routers (running up to Juniper Junos operating system 10.4); and Juniper standalone IDP Series appliances.

Juniper firewall products, including the SRX Series, can act as Layer 3 through Layer 7 overlay enforcement points for the Pulse Policy Secure. For organizations desiring Layer 2 port- based enforcement, support for vendor-agnostic 802.1X switches and wireless access points by Pulse Policy Secure enables them to quickly realize the benefits of NAC without requiring a hardware overhaul. Also, it supports branch SRX Series gateways, including the Juniper Networks SRX100, SRX110, SRX210, SRX220, SRX 240, SRX650 and virtual appliances such as Firefly Perimeter Services Gateways as 802.1X RADIUS clients, saving cost as well as providing 802.1X support for branch offices.

The EX Series switches[3] can allow you to manage security and access control policies from a centralized PSA Series Appliance Family running Pulse Policy Secure. Whenever a device completes 802.1X or MAC authentication, Pulse Policy Secure will push a user/ role-based authentication table entry to the EX Series switches, which will dynamically provision an access control list (ACL) to the switch port for that particular device. This alleviates the need for administrators to create hundreds of ACLs statically on individual switches, saving time and cost. Pulse Policy Secure and EX Series switches also allow centralized management for Web authentication. When a user connects to an EX Series switch port that has been enabled for Web authentication, the EX Series switch will perform a URL redirect to a PSA Series or MAG Series appliance running Pulse Policy Secure, which will return a captive portal authentication page to the user. And, with Pulse Policy Secure and EX Series switches, administrators no longer need to pre-provision switch ports to be dedicated for a specific purpose. Instead, all EX Series switch ports are configured with a shared policy, and the combination of Pulse Policy Secure and the EX Series switch tailors authentication and access to whatever or whoever is attaching to the port, significantly increasing usability and simplifying administration. Also, EX Series switches can apply quality of service (QoS) policies or mirror user traffic to a central location for logging, monitoring, or threat detection with IPS.

J Series routers may also serve as Layer 2 policy enforcement points. (J Series routers running Junos OS 10.4 or earlier may also serve as Layer 3 enforcement points for Pulse Policy Secure .)

With SRX Series gateways with intrusion prevention system delivering coordinated threat control, and standalone IDP Series appliances serving as role-based, application-level policy enforcement points, Pulse Policy Secure delivers granular identity- and role-based, access control to, and visibility into the application layer within your network. Also, Pulse Policy Secure coupled with SRX Series gateways enables user role- based AppSecure policies. Pulse Policy Secure and the SRX Series[4] enable the configuration of application-aware firewall policies based on an authenticated user's role in Pulse Policy Secure, empowering deployed SRX Series gateways to utilize the user's role information for the application of granular policies for application access based on a specific user's identity.

Many Juniper firewalls also support Unified Threat Management (UTM) capabilities, including IPS functionality, network-based antivirus, antispam, anti-adware, antiphishing, and URL filtering capabilities. This functionality can be dynamically leveraged as part of Pulse Policy Secure to enforce and unify access control and security policies on a per user and per session basis, delivering comprehensive network access and threat control. Pulse Policy Secure enforcement points, including the SRX Series gateways, may also be implemented in transparent mode, which requires no rework of routing and policies or changes to the network infrastructure. They may also be set up in audit mode to determine policy compliance without enforcement, enabling you and your users to ease into network access control (NAC).

[2]Running Junos OS 12.2 or higher

[4]Only for SRX Series gateways running Junos OS 12.1 or higher

Features and Benefits

Pulse Policy Secure is self-administering—intelligently quarantining noncompliant users and devices, and delivering extended remediation capabilities. It also provides automatic remediation for noncompliant devices, many times without user intervention or other assistance.

Table 1: Visibility

Feature	Feature Description	Benefits
On-box Pulse Secure Profiler	• Endpoint visibility into on-premise and remote connection via PCS • Fingerprinting Methods: DHCP Fingerprinting (Helper Address or RSPAN port), MAC OUI, SNMP/SNMP Traps, CDP/LLDP, HTTP User Agent, Nmap, WMI and MDM • Device Discovery Reporting & Dashboard with advanced filters and historical data • Standalone Profiler to support Active/Active cluster or non-cluster Pulse Policy Secure and Pulse Connect Secure deployment	• Collect endpoint device profiling information and maintain dynamic, contextual inventory of networked devices • View local and remote endpoints from single GUI • Monitor and manage devices for profile change • Supports comprehensive policy enforcement • Use device inventory for asset management • Useful for troubleshooting and visibility purpose • Support scalable cluster configuration with standalone profiler

Table 2: Advanced Network and Application Protection

Feature	Feature Description	Benefits
Role-based, application-level enforcement	• Leveraging Juniper SRX Series Firewalls as enforcement points enables context-based resource access control to be enforced via application specific policy rules • On the Juniper SRX Series Firewalls, policies can also be defined to control time-of-day and bandwidth restrictions per application or per role	• Enables access control and security policies to be applied to the application level, granularly protecting your network, applications, and data • Ensures that users adhere to application usage policies, controlling access to applications such as instant messaging, peer-to-peer, and other corporate applications
Automated patch assessment checks and remediation (optional)	• Can tie access directly to the presence or absence of specific hot fixes for defined operating systems and applications, and performs role-based, predefined patch management checks according to the severity level of vulnerabilities • Installed Systems Management Server (SMS) and/or System Center Configuration Manager (SCCM) 2007 can be leveraged to automatically check for patch updates, quarantining, remediating, and providing authorized network access once a device has been remediated	• Enables enhanced, granular endpoint device health and security state assessments • Minimizes user interaction and downtime through automatic remediation and management of patches for endpoint devices, reducing help desk calls
Coordinated threat control (CTC)	• Leverages robust features and capabilities of the SRX Series gateways for data center and branch, as well as the IDP Series appliances to deliver broad L2 through L7 visibility into application traffic isolating a threat down to the user or device level, and employing specific configurable policy action against the offending user or device	• Addresses and mitigates network insider threats quickly and simply • Minimizes network and user downtime
Captive portal	• If a user attempts unauthorized network access via a Web browser, administrators have an option to redirect the user to a Pulse Policy Secure enabled PSA Series Appliance Family for authentication • Once the user logs into the PSA Series Appliance Family with appropriate credentials, Pulse Policy Secure and the PSA will redirect the Web browser back to the original resource from which it had been redirected	• Provides network access control for guests and contractors

Pulse Policy Secure correlates user identity and role information to network and application security and usage. With the Pulse Policy Secure, you will know who is accessing your network and applications, when your network and applications are being accessed, what is being accessed, and where the user has been on your network.

Features and Benefits (continued)

Table 3: Identity-Enabled Network and Application Control

Feature	Feature Description	Benefits
Federation	• Federation of user sessions between Pulse Connect Secure (SSL VPN) and the Pulse Policy Secure, both running on PSA Series Appliance Family, enables seamless provisioning of remote access user sessions into LAN access user sessions upon login, or alternatively LAN access user sessions into remote access user sessions at login • Allows a remote access user connected via SSL VPN to a PSA Series Appliance Family with Pulse Policy Secure to be granted seamless access to the LAN and its protected resources through a PSA Series Appliance Family running Pulse Policy Secure, without needing to re-authenticate • Users authenticated to one Pulse Policy Secure-enabled PSA Series Appliance Family may, if authorized, access resources protected by another Pulse Policy Secure-enabled PSA Series Appliance Family, enabling "follow-me" policies • Pulse Policy Secure leverages the TCG's Trusted Network Connect standard IF-MAP protocol to enable federation	• Offers a consistent user access experience • Enables location awareness and session migration capabilities in Pulse Secure Solution
Identity-enabled firewalls	• Combines identity-aware capabilities of Pulse Policy Secure with the robust networking and security services of the SRX Series Firewalls, Palo Alto Networks and Fortinet Firewalls[5], enabling SRX Series, Palo Alto Networks and Fortinet Firewalls to be employed as policy enforcement points	• Drastically increases scalability for data center environments and branch offices alike
User role-based AppSecure policies	• Configures application-aware Firewall policies in SRX Series firewalls based on the role of an authenticated user to Pulse Policy Secure • Empowers deployed SRX Series Firewalls to utilize user role information to apply granular policies for application access based on a specific user's identity	• Adds identity-awareness to application- aware firewall policies, delivering fi access control granularity
Mobile Device Management (MDM) Integration	• Allows for policy based on mobile device attributes and state collected from 3rd party MDM vendors such as MobileIron, AirWatch, Microsoft Intune and Pulse Workspace solutions • Enables virtually transparent deployment of fully configured Pulse Clients for simplified mobile SSL VPN connectivity • Consolidates mobile device and policy management controls reducing operational complexity	• Reduces complexity and increases policy intelligence to simplify and secure BYOD efforts for both IT and end-users

Pulse Policy Secure provides standards-based, vendor-agnostic access control and seamless support for existing, heterogeneous network environments. It leverages industry standards that include RADIUS, IPsec, and innovative, open standards such as the TNC's standards for network access control and network security. Pulse Policy Secure has been built on industry-leading products, including the policy engine, AAA, and Host Checker capabilities of PSA Series Appliance Family, as well as the RADIUS capabilities from SBR (Steel-Belted Radius) Enterprise Servers.

[5]Available on all SRX Series Services Gateways running Junos OS 9.4 or higher

Features and Benefits (continued)

Table 4: Standards-Based, Interoperable Access Control

Feature	Feature Description	Benefits
TNC open standards support, including IF-MAP support and Windows SOH and embedded NAP Agent support (optional)	• Adopts and provides strong support for the TCG's TNC open standards for network access control and security • Adopts the TNC's open standard IF-MAP, enabling integration with third- party network and security devices, including devices that collect and (through IF-MAP) share information on the state and status of a network, user, or device • Pulse Policy Secure-enabled PSA or MAG Series Appliance can serve as Metadata Access Point (MAP) servers, enabling collected data to be used in formulating policies and appropriate access actions • Through the TNC SOH standard, leverages preinstalled Windows 10, Microsoft Windows 8.1, Windows 8, Windows RT, Windows 7, Windows Vista, clients for access control with the Pulse Access Control Service, allowing use of the Windows Security Center (WSC) SOH in access control decisions	• Empowers organizations to select endpoint and network security solutions that meet their needs without concern for interoperability • Enables ease of deployment, leading to faster ROI. • Integrates existing, third-party network and security devices into the access control platform. • Streamlines client deployment, simplifying access control rollout and implementation
EX Series switch interoperability	• EX2200, EX3200, EX4200, and EX8200 switches interoperate with and serve as enforcement points for Pulse Policy Secure—using standards- based 802.1X port-level access control and L2 through L4 policy enforcement • When deployed with Pulse Policy Secure-enabled PSA Series Family Appliance, EX Series switches can orchestrate policies and dynamically provision ACLs in conjunction with Pulse Policy Secure, allow and manage Web authentication via Pulse Policy Secure, configure all EX Series switch ports with a shared policy with tailored authentication and access to whatever or whoever is attaching to the port, and enforce user-based QoS policies or mirror user traffic to a central location for logging, monitoring, or threat detection	• Delivers a complete, standards-based, best-in-class access control solution, allowing organizations to enjoy value-added features and economies of scale for support and service
Support for RADIUS CoA	• Without starting entire process of authentication, RADIUS CoA allows devices to change the VLAN/ACL for the endpoint based on roles	• Provides expanded interoperability with Cisco, HP/ Aruba and Brocade/Ruckus network infrastructure. No firewall enforcement is required
SNMPv1/v2c/v3 Support	• Supports endpoint and network device Visibility with SNMP v1/v2c/v3. The endpoints are discovered through SNMP Traps and network devices are discovered with SNMP discovery mechanism • Pulse Policy Secure also support SNMP enforcement for MAC based authentication and role assignment. After MAC authentication, Layer 3 Pulse session used for comprehensive host checking capability	• Endpoint and Network Device Visibility • Ease of NAC deployment with SNMP enforcement based on compliance and role-base access • No need for 802.1x supplicant • Support hybrid NAC deployment (802.1x for wireless network and SNMP for wired network) • Reduce CAPEX by supporting legacy switches that do not support 802.1x feature

Pulse Policy Secure enables organizations to begin controlling network and application access quickly and simply. Organizations are encouraged to initiate network access control with the Pulse Policy Secure in a phased approach, beginning with a small deployment and growing to support hundreds of thousands of concurrent users through its unparalleled scalability.

Features and Benefits (continued)

Table 5: Simple, Flexible Deployment

Feature	Feature Description	Benefits
Guest access support	• Onetime guest user accounts are available • Guest user accounts may also be provisioned with a predefined timeout period. • Administrators control the maximum time duration allowed • Reception and other nontechnical enterprise employees can host/provision secure guest user accounts dynamically through easy-to-use guest user account management • Bulk account creation can be used to create a large number of guest user accounts. • The ability to send guest user credentials via e-mail to an expected guest user simplifies guest account creation	• Enhances and simplifies an organization's ability to provide secure, differentiated guest user access to its network and resources
Centralized policy management	• Common configuration templates can be shared between Pulse Connect Secure (remote access control) and Pulse Policy Secure (network access control) deployments using Juniper Networks Network and Security Manager • NSM also provides a single management server that can configure key components of a Pulse Policy Secure deployment	• Saves administrative time and cost, and offers a consistent user and administrative experience by delivering common remote and local access control policy implementation and enforcement across a distributed enterprise • Makes possible and simplifies enterprise-wide deployment of uniform access control policies
Common access licensing	• Only requires user licenses (with appropriate Pulse PSA Series Appliance Family) to initiate access control • User licenses can either be used for concurrent user sessions with Pulse Policy Secure or Pulse Connect Secure	• Simplifies the product licensing model that can be used across NAC and SSL VPN deployments Note: Please see the Ordering Information section for the new common access license SKUs that can now be used for Pulse Policy Secure and Pulse Connect Secure
Wizard-based configuration	• An optional, step by step configuration wizard to aid administrators in the configuration of five of the most common deployment scenarios, including: • System setup • RADIUS configuration • Guest user management • L2 enforcement • L3 enforcement • Tasks for a given deployment scenario are arranged in a well-defined, dependent order • Wizard-based configuration admin UI navigates to the corresponding configuration screen when the administrator clicks on a particular task	• Aids administrators in navigating and familiarizing themselves with configuration tasks in Pulse Policy Secure admin UI
Intutitive dashboard	New dashboard design provides: • System overview - system information, licenses used, total users, critical events, etc. • Activity - Appliance statistics, authentication success/failure, compliance results, realms, etc. • Active user and endpoint management	• The rich data representation of endpoints visibility, activity monitoring and system overview enables administrators to quickly analyze and troubleshoot overall network security posture assessment
Dynamic authentication policy	• Leverages an organization's existing investment in directories, Public Key Infrastructure (PKI), and strong authentication • Supports 802.1X, RADIUS, Lightweight Directory Access Protocol (LDAP), Microsoft Active Directory, SQL (Oracle), RSA Authentication Manager, Network Information Service (NIS), certificate servers (digital certificates/PKI), local login/password, CA SiteMinder, RSA ClearTrust, and RADIUS Proxy • Supports RADIUS CoA (Change of Authorization) Change the attributes of an authentication, authorization, and accounting session during re-authentication process	• Saves time and expense by leveraging and interfacing with existing AAA infrastructures • Establishes a dynamic authentication policy for each user session • Enables support—through RADIUS proxy—for deployments where certain authentications are supported by a backend RADIUS server • Provides expanded interoperability with Cisco, HP/Aruba and Brocade/Ruckus network infrastructure. Without starting entire process of authentication, RADIUS CoA allows devices to change the VLAN/ACL for the endpoint based on roles. No firewall enforcement is required
Dynamic addressing of unmanageable endpoint devices	• Employs media access control (MAC) address authentication via RADIUS, in combination with MAC address whitelisting and blacklisting; or, leverages existing policy and profile stores (through LDAP interfaces) or asset discovery or profiling solutions for role- and resource-based access control of unmanageable devices such as networked printers, cash registers, bar code scanners, VoIP handsets, etc.	• Enhances network and application protection • Makes it simpler and faster for organizations to deploy access control across their entire network regardless of device manageability • Saves time and cost
Pulse Secure/ Pulse Policy Secure localization	• Provides localized UI, online help, installer, and documentation for Pulse Secure, supporting the following languages: - Chinese (Simplified) - German - Chinese (Traditional) - Japanese - English - Korean - French - Spanish	• Enables organizations to effectively deploy Pulse Policy Secure worldwide.
Granular auditing and logging	• Provides fine-grained auditing and logging capabilities, including access to Pulse Policy Secure RADIUS diagnostic log files, delivered in a clear, easy to understand format • Captures detailed logging by the roles that users belong to, resources that they are trying to access, and the state of compliance of the endpoint and user to the security policies of the network	• Simplifies the diagnosis and repair of network issues that arise • Addresses industry and government regulatory compliance and audits
RADIUS only appliance (optional)	• Optional license enables some Pulse PSA Series Appliance Family to be deployed as RADIUS only appliances, using many of the features and functions found within the SBR Enterprise Series servers as a basis for its AAA and RADIUS capabilities	• Enables an organization to become familiar with the Pulse PSA Series Appliance Family and Pulse Policy Secure • Allows an organization to upgrade to a full featured Pulse Policy Secure license at a future date

Product Options

There are several licensing options available for Pulse Policy Secure.

Table 6: Product Licenses and Options

Product Licenses	Product License Description	Supported Appliances
Common access licenses	· With the Pulse PSA Series Appliance Family, common access licenses are available as user licenses. With common access licensing, licenses can either be used for Pulse Policy Secure (NAC) user sessions, or Pulse Connect Secure (SSL VPN) user sessions. Please refer to the Ordering Information section for more details · For administrative ease of use, each license enables as many users as specified, and licenses are additive. For example, if a 100 user license was originally purchased and the concurrent user count grows over the next year to exceed that amount, simply adding another 100 user license to the system will allow support for up to 200 concurrent users. The maximum number of common access licenses for Pulse Policy Secure and Pulse Connect Secure varies per Pulse PSA Series Appliance Family	PSA300, PSA3000, PSA5000, PSA7000c/f
Enterprise licenses	· Enterprise licenses allow any organization with one or more Pulse PSA Series Appliance Family to easily lease user licenses from one firewall to another, as required to adapt to changing organizational needs. The centralized licenses can be either perpetual or subscription licenses. Perpetual licenses feature a onetime charge; however, maintenance is an additional cost and an additional license is required to allow each Pulse PSA Series Appliance Family to participate in leasing · Subscription licenses offer a more flexible and overall valuable option with one, two, or three-year terms. Subscription licensing requires a licensing server, either dedicated or partially dedicated. (Please note that the licensing server does require a hardware maintenance contract)	PSA300, PSA3000, PSA5000, PSA7000c/f
IF-MAP server licenses	· Leveraging the TNC's IF-MAP specification, a Pulse PSA Series Appliance Family with Pulse Policy Secure (as a standalone or in a cluster) may operate solely as a MAP server with no additional concurrent user licenses · In this mode, the Pulse PSA Series Appliance Family with Pulse Policy Secure must have a MAP server license installed · Mixed Pulse PSA Series Appliance Family and MAP server mode is defined as any Pulse PSA Series Appliance Family with Pulse Policy Secure that simultaneously acts as both a Pulse PSA Series Appliance Family with Pulse Policy Secure and as a MAP server, where a concurrent user license has been installed. In this case, the MAP server license is not required on that Pulse PSA Series Appliance Family	PSA300, PSA3000, PSA5000, PSA7000c/f
Pulse Secure Profiler licenses	· This license enables organizations to detect and classify managed and unmanaged devices (local or remote) on the network for a complete visibility. It also enables RADIUS server functionality for AAA/ RADIUS services running on Pulse PSA Series Appliance Family	PSA-300, PSA3000, PSA5000, PSA7000c/f
OAC-ADD-UAC licenses	· This license enables Pulse Policy Secure support to be added to existing Juniper Networks Odyssey Access Client licenses, enabling OAC to be used as the agent/supplicant for Pulse Policy Secure	PSA300, PSA3000, PSA5000, PSA7000c/f
Role-based licenses	· With the Pulse PSA Series Appliance Family, Policy Secure licenses are available as user licenses. Please refer to the Ordering Information section for more details · For administrative ease of use, each license enables as many users as specified, and licenses are additive. For example, if a 100 user license was originally purchased and the concurrent user count grows over the next year to exceed that amount, simply adding another 100 user license to the system will allow support for up to 200 concurrent users. The maximum number of Policy Secure license varies per Pulse PSA Series Appliance Family	PSA300, PSA3000, PSA5000, PSA7000c/f
Juniper SRX Series role-based firewall license	· Juniper SRX Series role-based firewall license enables application-aware firewall policies between Pulse Policy Secure and the Juniper SRX Series Firewalls · Fully capable without the use of common access licenses, this feature provides a cost-effective solution to secure specific applications within the network (typically the data center) by allowing Pulse Policy Secure (running on a Pulse PSA Series Appliance Family) to let its identity-based list of user roles be accessed by the SRX Series Firewalls · The end user benefits from a seamless experience, unaware that Pulse Policy Secure exists, thanks to the integrated Windows domain single sign-on (SSO) functionality via Active Directory	PSA300, PSA3000, PSA5000, PSA7000c/f

Specifications

Pulse Secure client, as the user interface for Pulse Policy Secure, supports Microsoft Windows 10, Windows 8, Windows 8.1 Windows 7, Windows RT and Windows Vista SP2 operating systems. Pulse Secure also supports Apple Mac OS X 10.6 (or higher) operating system software, Apple iOS, and Google Android.

Clientless mode secures devices running Microsoft Windows 10, Windows 8.1, Windows 8.0, Windows 7, and Windows Vista SP2 operating systems, Apple Mac OS, and Linux operating systems and platforms including Fedora, Ubuntu and openSUSE, interoperating with supported browsers which include Microsoft Internet Explorer, Mozilla Firefox, and Apple Safari.

For specific supported operating system software, operating platforms, and browser versions, please refer to the latest version of the Pulse PSA Series Appliance Family document, which may be found at www.pulsesecure.net.

PSA Series Licensing Options

Ordering Number	Description
Policy Secure Licenses	
POLSEC-xU(-zYR)	Add x simultaneous PPS 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)
POLSEC-ADD-yU	Add y simultaneous PPS 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
PS-PROFILER-RADIUS-SM	Pulse Secure Profiler with max 500 devices for PSA 300/3000 Platform - Includes RADIUS Server capability
PS-PROFILER-RADIUS-MD	Pulse Secure Profiler with max 10,000 devices for PSA5000, PSA7000 Platform - Includes RADIUS Server capability
PS-PROFILER-RADIUS-LG	Pulse Secure Profiler with max 50,000 devices for PSA7000 Platform - Includes RADIUS Server capability
PS-PROFILER-RADIUS-SM-HA	Pulse Secure Profiler with max 500 devices for PSA300/3000 Platform - Includes RADIUS Server capability and High Availability
PS-PROFILER-RADIUS-MD-HA	Pulse Secure Profiler with max 10,000 devices for PSA5000 Platform - Includes RADIUS Server capability and High Availability
PS-PROFILER-RADIUS-LG-HA	Pulse Secure Profiler with max 50,000 devices for PSA7000 Platform - Includes RADIUS Server capability and High Availability
PS-PROFILER-RADIUS-SM-1YR or 2 YR or 3 YR	Pulse Secure Profiler with max 500 devices for PSA300/3000 or Virtual Platforms - Includes RADIUS Server capability and High Availability (Subscription 1 or 2 or 3 Year with GOLD Support)
PS-PROFILER-RADIUS-MD-1YR or 2YR or 3YR	Pulse Secure Profiler with max 10,000 devices for PSA5000 or Virtual Platforms - Includes RADIUS Server capability (Subscription 1 or 2 or 3 Year with GOLD Support)
PS-PROFILER-RADIUS-LG-1YR or 2YR or 3YR	Pulse Secure Profiler with max 50,000 devices for PSA7000 or Virtual Platforms - Includes RADIUS Server capability (Subscription 1 or 2 or 3 Year with GOLD Support)

Pulse Secure Services and Support

Pulse Secure is the leader in performance-enabling services that are designed to accelerate, extend, and optimize your high-performance network. Our services allow you to maximize operational efficiency while reducing costs and minimizing risk, achieving a faster time to value for your network. Pulse Secure ensures operational excellence by optimizing the network to maintain required levels of performance, reliability, and availability.

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 the company's Pulse virtual private network (VPN), network access control (NAC) and mobile security products to enable end user mobility securely and seamlessly in their organizations. Pulse Secure's mission is to enable open, 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