Pulse Secure

Pulse Policy Secure

Data Sheet

Published Date **July 2015**

Product Overview

Pulse Policy Secure is a market leading network and application access control (NAC) solution that ensures network access only to authorized and secured users and devices, protecting the network, core assets, applications, data and more—today and into the future.

Pulse Policy Secure delivers simple, secure network and application access control with a standards-based, granular solution that provides access control based on user identity, device type, integrity, and location.

Pulse Policy Secure supports phased deployment and can scale to support global distributed enterprises and service providers.

Your ideas. Connected.™

Product Description

Pulse Secure ® Pulse® Policy Secure[1], delivers granular, secure, identityenabled, location- and device-based access control for even the most complex network, cloud, and application 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 access control, and simplifying deployment, administration, and management.

The Pulse Policy Secure combines user identity, device type and security state, and device location data to create a unique, dynamic access control policy per user and per session. Through its incorporation of different levels of session-specific policy, the Pulse Policy Secure develops extremely granular access controls that are easy to deploy, maintain, and dynamically modify.

The Pulse Policy Secure can be enabled at Layer 2 leveraging 802.1X; at L3 using an overlay deployment; or in a mixed mode using 802.1X for network admission control and a L3 overlay deployment for resource access control. It fully integrates with any vendor's 802.1X-enabled wireless access points, such as the Juniper Networks WLA Series Wireless LAN Access Points and AX411 Wireless LAN Access Point; or any vendor's 802.1X-enabled switches, such as Juniper Networks EX Series Ethernet Switches, which, when deployed with the Pulse Policy Secure, deliver additional, rich policy enforcement capabilities. Existing 802.1X infrastructure may be leveraged, as well as any Juniper firewall platform such as the Juniper Networks SRX Series Services Gateways, for policy enforcement and granular access control. Pulse Policy Secure also supports the Juniper Networks J Series Services Routers as Layer 2 policy enforcement points. Pulse Policy Secure supports branch SRX Series gateways, allowing them to configure Pulse Policy Secure as a RADIUS server, saving cost while addressing 802.1X support for branch offices.

[1]Formerly known as Pulse Secure Unified Access Control

Network Security and Application Access Control Integration

The 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. The Pulse Policy Secure ties user identity and role information to network and application access, addressing regulatory compliance and audit demands. It also provides the ability to configure application-aware firewall policies based on the role of an authenticated user, empowering deployed SRX Series gateways as Pulse Policy Secure policy enforcement points to utilize the user's role information for the application of granular application access policies based on a specific user's identity. Pulse Policy Secure also supports L2 through L7 policy enforcement, offering unparalleled visibility into application traffic at L7 by leveraging SRX Series gateways for the data center, and standalone IDP Series devices as policy enforcement points.

Also, Pulse Policy Secure, deployed in conjunction with SRX Series gateways,[2] provides the ability to configure application-aware firewall policies based on the role of an authenticated user defined in the Pulse Policy Secure. This empowers customers with deployed SRX Series gateways to utilize the user's role information for the application of granular policies for application access based on the specific user's identity.

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.

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

Federation

The Pulse Policy Secure enables the federation— or sharing—of user session data between it and the Pulse Secure's 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. This enables a remote access user connected via SSL VPN to the Pulse Connect Secure to be granted seamless access to the LAN through the same or different Pulse Policy Secure instances, without reauthentication No reauthentication is required, enabling "follow-me" policies regardless of the user's device or worldwide location.

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

Guest Access

The Pulse Policy Secure offers optional, enhanced guest user access control capabilities to deliver secure, authorized network resource access for guests, partners, and contractors. It manages network use, and reduces threats from unauthorized users and compromised devices. It also enables enterprise selected and approved guest user account managers to provision temporary guest access accounts for corporate guest users, to create bulk accounts for numerous guest users, and to send guest user credentials via e-mail to an expected guest user, simplifying guest account creation.

Anti-Malware Protection and Patch Assessment

An optional Pulse Policy Secure license provides industry-leading, dynamic, anti-malware and antispyware protection for endpoint devices attempting network access. Pulse Policy Secure also offers device patch assessment checks, including endpoint inspection for targeted operating system or application hot fixes, with optional patch remediation services 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, the 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 8.1, Windows 8, Windows 7, Windows RT, Windows Vista, and/or Windows XP SP3 clients. The 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 the Pulse Policy Secure is deployed quickly and easily. Pulse Policy Secure 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. Also, SRX Series gateways can be deployed in transparent mode with Pulse Policy Secure.l
Service, simply acting as a "bump in the wire" (BITW), eliminating the need to modify your network's routing topology. Partner Mobile Device Management (MDM) systems such as those from MobileIron and Airwatch can be leveraged to transparently deploy and configure Pulse clients to Android and iOS devices facilitating deployment efforts to remote devices.

Architecture and Key Components

Pulse Policy Secure uses three core components to deliver identity-, location-, and device-aware network and application access control:

MAG Series Pulse Gateways

Pulse Policy Secure is the network and application access control software which runs both on the MAG Series Pulse Gateways and as a virtual machine over KVM or VMWare hypervisors. MAG Series gateways are purpose-built, centralized policy management servers that work with Pulse or in clientless mode to obtain user authentication, device security posture, and device location data from a user's endpoint device. This data to creates dynamic policies that are propagated to policy enforcement points throughout the distributed network worldwide.

Pulse Policy Secure leverages the policy control engine from Juniper's market-leading SSL VPN gateways, as well as their ability to seamlessly integrate with existing authorization, authentication, and accounting (AAA) and identity and access management (IAM) infrastructure. It also integrate RADIUS capabilities and enhanced services from Pulse Secure SBR Enterprise Series Steel-Belted Radius Servers, to support an 802.1X transaction when a mobile or nonmobile device attempts network connection. The Pulse Policy Secure and MAG Series gateways may also be licensed as standalone RADIUS servers.

You may simply deploying a single MAG Series gateway running Pulse Policy Secure with your existing vendoragnostic 802.1X switches or wireless access points, including EX Series Ethernet Switches, WLA Series Wireless LAN Access Points, AX411 Wireless LAN Access Point, Juniper firewalls including the SRX Series, or J Series routers.

Pulse Client and Clientless Mode Deployments

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

Pulse or clientless mode collects user and device credentials, and assesses the device's security state. Pulse leverages and integrates with the native 802.1X supplicant available within Microsoft Windows to deliver comprehensive L2 access control. Pulse Policy Secure can also support native 802.1X supplicants on Apple Mac OS X and iOS, and Google Android devices for L2 authentication. Pulse, along with Pulse Policy Secure, also provides L3 authentication and IPsec tunneling with any Juniper Networks 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 includes Juniper's Host Checker functionality, enabling you to define policy that scans both mobile and nonmobile 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 and MobileIron 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 Secure SSL VPN gateway 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, a check to see whether or not Pulse Mobile Security Suite is loaded on the device, 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 the Juniper SSL VPN gateways and the Pulse Policy Secure via the TNC IFMAP protocol. Pulse then pushes the appropriate access policies for the user and mobile device to deployed Juniper firewalls such as the SRX Series gateways.

Pulse 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. Pulse Policy Secure 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 also integrates dynamic 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.

Pulse supports L2 and L3 authentication and device integrity assessments for devices running Microsoft Windows 7 Enterprise, Windows Vista (32- and 64-bit), and Windows XP operating systems. It also supports devices running Apple Mac OS X 10.6 (or higher) operating system software, and devices running Apple iOS or Google Android.

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 Networks firewall platform, including the SRX Series gateways; J Series Services Routers (running up to Juniper Networks Junos operating system 10.4); and Juniper standalone IDP Series appliances.

Juniper Networks firewall products, including the SRX Series, can act as L3 through L7 overlay enforcement points for the Pulse Policy Secure. For organizations desiring L2 port-based enforcement, support for vendor-agnostic 802.1X switches and wireless access points by the Pulse Policy Secure enables them to quickly realize the benefits of NAC without requiring a hardware overhaul. Also, Pulse Policy Secure 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 MAG Series 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 MAG Series gateway running Pulse Policy Secure, which will return a captive portal authentication page to the user. And, with Pulse Policy Secure and EX Series

3 Running Junos OS 12.2 or higher

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

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 L2 policy enforcement points.

(J Series routers running Junos OS 10.4 or earlier may also serve as L3 enforcement points for the 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, the 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 the 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 Networks 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 the 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).

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: Advanced Network and Application Protection

Feature	Feature Description	Benefits
Role-based, application-level enforcement	• Leveraging SRX Series gateways as enforcement points enables application-specific policy rules to be enforced via any level of policy granularity. • 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.

Feature	Feature Description	Benefits
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 end-point device health and security state assessments. • Minimizes user interaction and down-time through automatic remediation and management of patches for end-point 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 down-time.
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 MAG Series gateway for authentication. • Once the user logs into the MAG Series gateway with appropriate credentials, Pulse Policy Secure and the MAG Series will redirect the Web browser back to the original resource from which it had been redirected.	• Provides network access control for guests and contractors.

The 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.

Table 2: Identity-Enabled Network and Application Control, Visibility, and Monitoring

Feature	Feature Description	Benefits
Federation	• Federation of user sessions between the Pulse Connect Secure (SSL VPN) and the Pulse Policy Secure, both running on MAG Series gateways, 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 MAG Series gateway with the Pulse Connect Secure to be granted seamless access to the LAN and its protected resources through a MAG Series gateway running Pulse Policy Secure, without needing to reauthenticate. • Users authenticated to one Pulse Policy Secure-enabled MAG Series gate-way may, if authorized, access resources protected by another Pulse Policy Secure-enabled MAG Series gateway, 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.
Identity-enabled firewalls	• Combines identity-aware capabilities of Pulse Policy Secure with the robust networking and security services of the SRX Series Services Gateways5, en-abling SRX Series gateways 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 gateways based on the role of an authenticated user to Pulse Policy Secure. • Empowers deployed SRX Series gateways to utilize user role information to apply granular policies for application access based on a specific user's identity.	• Adds identity-awareness to applica-tion-aware firewall policies, delivering finer 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 solutions. • Enables virtually transparent deployment of fully configured Pulse Clients for simpli-fied mobile SSL VPN connectivity • Consolidates mobile device and policy management controls reducing operation-al complexity	• Reduces complexity and increases pol-icy intelligence to simplify and secure BYOD efforts (Bring Your Own Device) for both IT and end-users

The 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 industryleading products, including the policy engine, AAA, and Host Checker capabilities of SA Series SSL VPN Appliances, as well as the RADIUS capabilities from SBR Enterprise Series Steel-Belted Radius Servers.

Table 3: 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 MAG Series gateways 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 Microsoft Windows 8.1, Windows 8, Windows RT, Windows 7, Windows Vista, and XP SP3 clients for access control with the Pulse Policy Secure, al-lowing use of the Windows Security Center (WSC) SOH in access control decisions.	• Empowers organizations to select end-point 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 the 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 MAG Series gateways, EX Series switches can orchestrate policies and dynamically provision ACLs in con-junction 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 val-ueadded features and economies of scale for support and service.

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.

Table 4: 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 the Pulse Connect Secure (remote access control) and the Pulse Policy Secure (network access control) deployments using Pulse Secure 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 MAG Series gateways) to initiate access control. • User licenses can either be used for concurrent user sessions with the Pulse Policy Secure or the 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 the 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 the Pulse Policy Secure admin UI.

Feature	Feature Description	Benefits
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, Oblix (Oracle), and RADIUS Proxy.	• 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.
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 resourcebased 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/Pulse Policy Secure localization	• Provides localized UI, online help, installer, and documentation for Pulse, supporting the following languages: -- Chinese (Simplified) -- Chinese(Traditional) -- English -- French -- German -- Japanese -- Korean -- Spanish	• Enables organizations to effectively deploy Pulse and the Pulse Policy Secure worldwide.
Granular auditing and logging	• Provides fine-grained auditing and logging capabilities, including access to the Pulse Policy Secure RADIUS diagnostic log files, delivered in a clear, easy to under-stand 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 MAG4610, MAG6610, and MAG6611 gateways 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 MAG Series gateways 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 the Pulse Policy Secure.

Table 5: Product Licenses and Options

Product Licenses	Product License Description	Supported Gateways
Common access licenses	• With the MAG Series Pulse Gateways, common access licenses are available as user licenses. With common access licensing, licenses can either be used for Pulse Policy Secure 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 num-ber of common access licenses for Pulse Policy Secure and Pulse Connect Secure per MAG Series gateway and service module can be found in the MAG Series Pulse Gateways data sheet at **https://www.pulsesecure.net/products/**	MAG2600, MAG4610, MAG6610, MAG6611
Enterprise licenses	• Enterprise licenses allow any organization with one or more MAG Series gateways to easily lease user licenses from one gateway 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 MAG Series gateway 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.)	MAG2600, MAG4610, MAG6610, MAG6611

Product Licenses	Product License Description	Supported Gateways
Microsoft SOH licenses	• The licensing of the System Health Agent (SHA), System Health Verifiers (SHVs), and SOH protocols from Microsoft are addressed, and are all key components that enable the Pulse Policy Secure to support the Microsoft Windows SOH and embedded NAP Agent through the TNC SOH open and standardized protocol, IF-TNCCS-SOH.	MAG2600, MAG4610, MAG6610, MAG6611
MAP server licenses	• Leveraging the TNC's IF-MAP specification, a MAG Series 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 MAG Series with the Pulse Policy Secure must have a MAP server license installed. • Mixed MAG Series and MAP server mode is defined as any MAG Series gateway with Pulse Policy Secure that simulta-neously acts as both a MAG Series gateway with the 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 MAG Series gateway.	MAG4610, MAG6610, MAG6611
Enhanced Endpoint Security subscription licenses	• Enhanced Endpoint Security enables Pulse Policy Secure to offer antispy-ware/anti-malware functionality to ensure that Microsoft Windows endpoint devices are not running spyware or keyloggers. • Devices contaminated by spyware may be quarantined or have restricted end user access based on policy enforcement. • Pulse Policy Secure with Enhanced Endpoint Security scans an end-point's memory, registry, and load points for spyware and malware. • A base Pulse Policy Secure license includes a free Enhanced Endpoint Security user license for two (2) simulta-neous users, allowing users to "try before they buy." • Subscription licenses for additional Enhanced Endpoint Security users are available.	MAG2600, MAG4610, MAG6610, MAG6611

Product Licenses	Product License Description	Supported Gateways
SRX Series role-based firewall license	• The SRX Series role-based firewall license enables applicationaware firewall policies between the Pulse Policy Secure and the SRX Series Services Gateways. • 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 MAG Series gateway) to let its identity-based list of user roles be accessed by the SRX Series. • The end user benefits from a seamless experience, unaware that the Pulse Policy Secure exists, thanks to the integrated Windows domain single sign-on (SSO) functionality via Active Directory.	MAG2600, MAG4610, MAG6610, MAG6611
Automatic Patch Remediation license	• The Automatic Patch Remediation license combines a MAG Series gateway and Pulse Policy Secure with VMware's (formerly Shavlik) industry-leading asset discovery and broad update capabilities. • It provides an additional layer of security and control over unmanaged endpoints. • The Automatic Patch Remediation license enables MAG Series gateways to automatically scan Windows-based PCs and laptops for security threats, and perform remediation before granting users and their devices full access to the corporate network. • It does not require SMS or SCCM for remediation, and it addresses the latest operating system and software patches from Microsoft, as well as from other vendors such as Adobe Systems, Mozilla Firefox, Apache, RealPlayer, and others. • More information is available in the Automatic Patch Remediation License datasheet at **https://www.pulsesecure.net/products/**	MAG2600, MAG4610, MAG6610, MAG6611

Product Licenses	Product License Description	Supported Gateways
RADIUS only licenses	• This license give organizations that wish to deploy RADIUS appliance access to only the AAA/RADIUS features of the Pulse Policy Secure-enabled MAG Series gateways. • It introduces the organization to the MAG Series gateways and the Pulse Policy Secure, as well as allowing the organization to upgrade to a full featured Pulse Policy Secure license at a future date.	MAG4610, MAG6610, MAG6611
OAC-ADD-UAC licenses	• This license enables Pulse Policy Secure support to be added to exist-ing Pulse Secure Odyssey Access Client licenses, enabling OAC to be used as the agent/ supplicant for Pulse Policy Secure.	MAG2600, MAG4610, MAG6610, MAG6611

Specifications

Pulse client, as the user interface for Pulse Policy Secure, supports Microsoft Windows 8, Windows 8.1 Windows 7, Windows RT, Windows Vista SP2, and Windows XP SP3 operating systems. Pulse 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 7, Windows Vista SP2 , and Windows XP SP3 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 MAG Series Supported Platforms document, which may be found at **https://www.pulsesecure.net/techpubs/**

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. For more details, please visit **https://www.pulsesecure.net/products/.**

Ordering Information

Model Number	Description
MAG2600-LICENSE-MBR	Allows MAG2600 gateway to participate in leased licensing
MAG4610-LICENSE-MBR	Allows MAG4610 gateway to participate in leased licensing
SM160-LICENSE-MBR	Allows MAG SM160 gateway-blade to participate in leased licensing
SM360-LICENSE-MBR	Allows MAG SM360 gateway-blade to participate in leased licensing
Microsoft SOH License	
MAGX600-SOH	Adds Microsoft SOH/NAP Agent integration capabilities to the MAGX600 Pulse Gateway
MAP Server Licenses	
MAGX600-IFMAP	License for IF-MAP server on standalone MAG Series gateway with Pulse Policy Secure (hardware purchased separately)
Enhanced Endpoint Security Subscription Licenses	
ACCESS-EES-xU-zYR	Enhanced Endpoint Security subscription, x concurrent users, z-year x options: 100, 250, 500, 1,000, 2,500, 5,000, 7,500, 10,000, 15,000, 20,000, or 25,000 simultaneous users. Enhanced Endpoint Security user license count cannot exceed the number of user licenses/ common access licenses. z options: 1, 2, or 3 year subscription
SRX Series Role-Based Firewall Licenses	
MAGX600-UAC-SRX- 25U	Role-based firewall licenses for 25 users Basic Features
MAGX600-UAC-SRX- 250U	Role-based firewall licenses for 250 users Basic Features
MAGX600-UAC-SRX- 500U	Role-based firewall licenses for 500 users Basic Features
MAGX600-UAC-SRX- 5KU	Role-based firewall licenses for 5,000 users Basic Features
MAGX600-UAC-SRX- 15KU	Role-based firewall licenses for 15,000 users Basic Features

Ordering Information

Model Number	Description
Automatic Patch Remediation License Options	
ACCESS-PRM-xU-zYR	Patch Remediation Management (PRM), z-year subscription for x simultaneous users x options: 50, 100, 250, 500, 1,000, 2,000, 2,500, 5,000, 7,500, 10,000, 20,000 or 25,000 simultaneous users. PRM user license count cannot exceed the number of user licenses/common access licenses. z options: 1, 2, or 3 year subscription
ACCESS-PRM-xU-zYR-R	Patch Remediation Management (PRM), z-year subscription renewal for x simultaneous users x options: 50, 100, 250, 500, 1,000, 2,000, 2,500, 5,000, 7,500, 10,000, 20,000 or 25,000 simultaneous users. PRM user license count cannot exceed the number of user licenses/common access licenses. z options: 1, 2, or 3 year subscription
Radius License Only	
MAGX600-RADIUS-SERVER	Add RADIUS Server Feature to the MAGX600
OAC-ADD-UAC Licenses	
MAGX600-OAC-ADD-UAC	Allows Windows edition OAC clients to be converted to the UAC edition OAC clients (UAC Agents) and used with MAGX600 Pulse Gateway

About Pulse Secure

Pulse Secure is in the business of network innovation. From devices to data centers, from consumers to cloud providers, Pulse Secure delivers the software, silicon and systems that transform the experience and economics of networking. The company serves customers and partners worldwide. Additional information can be found at **www.pulsesecure.net.**

Pulse Secure, LLC
2700 Zanker Road, Suite 200
San Jose, CA 95134