JUNOS PULSE SECURE ACCESS SERVICE

Product Overview

Employees are more mobile than ever before, and they carry multiple company issued and personal (BYOD) computing devices. They want fast, easy yet secure mobile and remote access that empowers them to do their jobs effectively. One of the key Junos Pulse services, Junos Pulse Secure Access Service provides cost-effective, secure, authenticated access via SSL VPN for remote and mobile users from any web-enabled device to corporate resources—anytime, anywhere.

Product Description

Enterprises and service providers have the difficult challenge of providing location- and device-independent network connectivity that is secure and capable of controlling resource access for authorized users. Breaches and threats continue to spiral out of control, and increasing numbers of employees and users want to use their own personal mobile and computing devices to access enterprise data and applications, making this challenge even more difficult. Juniper Networks® Junos® Pulse Secure Access Service provides secure, authenticated access for remote and mobile users from any web-enabled device to corporate resources—anytime, anywhere. The Junos Pulse Secure Access Service is a leading, most widely deployed SSL VPN, and the remote access standard for organizations of any size, across every major industry.

Junos Pulse Secure Access Service includes Juniper Pulse clients and the AppConnect SDK. Junos Pulse clients are dynamic, multiservice network client for mobile and personal computing devices. Junos Pulse clients are simply deployed, enabling users to quickly "click and connect" from any device, anywhere. Junos Pulse Junos Pulse AppConnect SDK delivers per-application SSL VPN connectivity for iOS and Android clients, enabling IT to create an even more transparent and secure mobile app experience for their users.

For more details on Junos Pulse, please visit **www.juniper.net/us/en/products-services/software/junos-platform/junos-pulse**.

Architecture and Key Components

Junos Pulse Secure Access Service can be enabled as both hardware-based MAG Series gateways and as Contrail-ready virtual appliances.

- **MAG2600 Junos Pulse Gateway**: Fixed configuration appliance ideal for small and mid-size businesses, supporting up to 100 SSL VPN concurrent users.
- **MAG4610 Junos Pulse Gateway:** Fixed configuration appliance ideal for mid-size and large businesses, supporting up to 1,000 SSL VPN concurrent users.
- **MAG6610 Junos Pulse Gateway:** Chassis-based appliance ideal for scalable large businesses, the MAG6610 can support up to 20,000 SSL VPN concurrent users; it requires at least one service module (maximum of two) to be ordered and installed (MAG-SM160 or MAG-SM360).
- **MAG6611 Junos Pulse Gateway:** Chassis-based appliance ideal for meeting the highest scalability needs of large businesses, the MAG6611 can support up to 40,000 SSL VPN concurrent users; it requires at least one service module to be ordered (maximum of four) and installed (MAG-SM160 or MAG-SM360).

- **Virtual Appliance:** VMWare and KVM virtual appliances for scalable elastic deployment of SSL VPN services

For more details on MAG Series hardware, including the specifications and ordering information of each model, please refer to the MAG Series Junos Pulse Gateways datasheet.

Features and Benefits

Junos Pulse Mobile Clients

Junos Pulse clients securely connect users to networks. Wrapped in an extremely user-friendly package, Junos Pulse dynamically enables the appropriate network and security services on users' endpoints. Users are not distracted from their work activities to figure out what network they are on or what service to enable. With Junos Pulse, the connection just works, helping to deliver the productivity promised by mobile devices. Junos Pulse delivers dynamic access control, seamlessly switching between remote (SSL VPN) and local (UAC) access control services on Microsoft Windows devices. Junos Pulse also enables comprehensive endpoint assessment for mobile and computing devices, and quarantine and remediation, if necessary.

Table 1: Key Features of Junos Pulse Secure Access Service

Feature	Feature Description
Layer 3 SSL VPN	• Dual-transport (SSL + Encapsulating Security Payload) full Layer 3 VPN connectivity with granular access control.
Application VPN	• Client/server proxy application that tunnels traffic from specific applications to specific destinations (available for Windows devices only).
Ease of use	• Seamless roaming from remote access to local LAN access (available for Windows devices only).
Endpoint integrity and assessment	• Assess and remediate end user devices prior to authentication with easy policy definition. Available on Windows, Mac OS X, Apple iOS, Android, and Windows Mobile 6.5 (capabilities vary by platform). Available pre-installed with Microsoft Windows 8.1 and RT.
Split tunneling options	• Full range of split tunneling options are configurable. • Includes enable and disable functionality with overriding route capability and route monitoring. • Pulse AppConnect enables IT to integrate per-application SSL VPN connectivity for maximum data security and user transparency.
Flexible launch options (standalone client, browser-based launch)	• Users can easily launch SSL VPN via their Web browser, or directly from their desktop.
Preconfiguration options (Windows and Mac only)	• Administrators can preconfigure a Junos Pulse deployment with a list of gateways for end users to choose from.
Authentication options (hardware token, smart cards, or soft token)	• Administrators can deploy Junos Pulse for remote user authentication using a wide array of authentication mechanisms, including one-time passwords and certificate authentication.
Layer 7 Web single sign-on (SSO) via SAML	• Allows end users to authenticate to the network through a Layer 3 tunnel, while simultaneously enjoying SSO to Web applications accessed through their browser via SAML SSO support.

For more details on Junos Pulse, please visit **www.juniper.net/us/en/products-services/software/junos-platform/junos-pulse/**.

End-to-End Layered Security

Junos Pulse Secure Access Service provides complete end-to-end layered security, including endpoint client, device, data, and server layered security controls.

Table 2: End-to-End Layered Security Features and Benefits

Feature	Feature Description	Benefits
Host Checker	• Endpoint devices can be checked prior to and during a remote access session to verify an acceptable device security posture requiring installed/running endpoint security applications (antivirus, personal firewall, etc.). • Custom-built checks for specialized customer requirements are also supported. • Noncompliant endpoints can be quarantined, denied access, or granted access, depending on administrator defined policies. • Whenever possible, Host Checker automatically remediates noncompliant endpoints by updating software applications that do not comply to corporate security policies.	• Ensures that endpoint devices meet corporate security policy requirements before being granted network access. • Remediates devices and quarantines users, when necessary. • Also ensures that no potentially sensitive data is left behind on the endpoint device.

Table 2: End-to-End Layered Security Features and Benefits (continued)

Feature	Feature Description	Benefits
Trusted Network Connect (TNC) support in Host Checker	• Allows interoperability with diverse endpoint security solutions from antivirus to patch management to compliance management solutions.	• Enables customers to leverage existing investments in endpoint security solutions from third-party vendors.
Security services with kernel-level packet filtering and safe routing	• Undesirable traffic is dropped before it is processed by the TCP stack.	• Ensures that unauthenticated connection attempts such as malformed packets or denial-of-service (DoS) attacks are filtered out.
Secure virtual workspace	• A secure and separate environment for remote sessions which encrypts all data and controls I/O access (printers, drives).	• Ensures that all corporate data is securely deleted from unsecure kiosks after a remote access session.

Ease of Administration

In addition to enterprise-class security benefits, the Junos Pulse Secure Access Service has a wealth of features that make it easy for the administrator to deploy and manage.

Table 3: Ease of Administration Features and Benefits

Feature	Feature Description	Benefits
Mobile Device Management (MDM) integration (Including AirWatch and MobileIron)	• Enables consolidated reporting and dashboards for simplified management • Leverages of MDM attributes for more intelligent and centralized policy creation • Facilitates transparent "no touch" MDM-based deployment of Pulse clients to iOS and Android devices	• Existing directory investments can be leveraged with no infrastructure changes and no APIs for directory.
Integration with strong authentication and identity and access management (IAM) platforms	• Ability to support SecurID, Security Assertion Markup Language (SAML) including standards-based SAML v2.0 support, and public key infrastructure (PKI)/digital certificates.	• Leverages existing corporate authentication methods to simplify administration.
Bridge Certification Authority (BCA) support	• Supports federated PKI deployments with client certificate authentication. Bridge CA is a PKI extension (as specified in RFC 5280) to cross-certify client certificates that are issued by different trust anchors (Root CAs). • Also, enables customers to configure policy extensions in the admin UI, to be enforced during certificate validation.	• Enables customers who use advanced PKI deployments to deploy the MAG Series Junos Pulse Gateways to perform strict standards-compliant certificate validation—before allowing data and applications to be shared between organizations and users.
Multiple hostname support	• Ability to host different virtual extranet websites from a single appliance.	• Saves the cost of incremental servers. • Eases management overhead. • Provides a transparent user experience with differentiated entry URLs.
Customizable user interface	• Creation of completely customized sign-on pages.	• Provides an individualized look for specified roles, streamlining the user experience.
Juniper Networks Network and Security Manager	• Centralized management application for configuring, updating, and monitoring MAG Series Junos Pulse Gateways within a single device/cluster or across a global cluster deployment.	• Enables companies to conveniently manage, configure, and maintain MAG Series gateways and other Juniper devices from one central location.
Cross-platform support	• Ability for any platform – including Windows (including Windows 8), Mac OS (including OS X 10.8/Mountain Lion), Linux, and various mobile operating systems such as iOS, Windows Mobile, Symbian, and Android – to attempt and if authenticated and authorized, to gain remote access to networked resources.	• Provides flexibility in allowing users to access corporate resources from any type of device using any type of operating system.
Enterprise licensing	• Allows any organization with one or more devices to group licenses and flexibly distribute across devices as capacity needs change over time.	• Provides flexible license capacity per device, allowing for changes as required by usage patterns.

Rich Access Privilege Management Capabilities

Junos Pulse Secure Access Service provides dynamic access management capabilities. When users log into MAG Series gateways running Junos Pulse Secure Access Service, they pass through a pre-authentication assessment, and are then dynamically mapped to the session role that combines established network, device, identity, and session policy settings. Users have access only to those resources that are deemed necessary for that session, according to administrator-defined policies.

Table 4: Access Privilege Management Features and Benefits

Feature	Feature Description	Benefits
Dynamic role mapping with custom expressions	• Combines network, device, and session attributes to determine which types of access are allowed. • A dynamic combination of attributes on a per-session basis can be used to make the role mapping decision.	• Enables the administrator to provision by purpose for each unique session.
Resource authorization	• Provides extremely granular access control to the URL, server, or file level for different roles of users.	• Allows administrators to tailor security policies to specific groups, providing access only to essential data.
Granular auditing and logging	• Can be configured to the per-user, per-resource, per-event level for security purposes as well as capacity planning.	• Provides fine-grained auditing and logging capabilities in a clear, easy to understand format.
UAC-SSL VPN federation	• Seamlessly provision SSL VPN user sessions into UAC sessions upon login, or the alternative (provisioning of UAC sessions into SSL VPN sessions). • Since session data is shared between the Juniper Networks gateways or appliances for SSL VPN and UAC, users need to authenticate only one time to get access in these types of environments.	• Provides users, whether remote or local, seamless access with a single login to corporate resources that are protected by access control policies. • Simplifies the end user experience.
Multiple sessions per user	• Allows remote users to launch multiple remote access sessions.	• Enables remote users to have multiple authenticated sessions open at the same time, such as when accessing VPN from a laptop and from a smartphone simultaneously.
User record synchronization	• Supports synchronization of user records such as user bookmarks across different non-clustered MAG Series gateways running Junos Pulse Secure Access Service.	• Ensures a consistent experience for users who often travel from one region to another and therefore need to connect to different MAG Series gateways running Junos Pulse Secure Access Service.
Mobile-friendly SSL VPN login pages	• Provides predefined HTML pages that are customized for mobile devices, including Apple iPhone and iPad, Google Android, and Nokia Symbian devices.	• Provides mobile device users with a simplified and enhanced user experience and webpages customized for their device types.

Flexible Single Sign-On (SSO) Capabilities

Junos Pulse Secure Access Service for the MAG Series Junos Pulse Gateways offers comprehensive single sign-on (SSO) features. These features increase end user productivity, greatly simplify administration of large diverse user resources, and significantly reduce the number of help desk calls.

Table 5: Flexible Single SSO Features and Benefits

Feature	Feature Description	Benefits
SAML single sign-on for cloud and Web applications access	• SAML 2.0-based SSO to a variety of Web applications, including many of today's most popular Software as a Service (SaaS) applications such as salesforce.com and Google Apps. • Includes SSO functionality, even when connecting via a Junos Pulse Secure Access Service Layer 3 VPN tunnel, which is unique in the industry.	• Single sign-on to a user's Web and cloud-based applications, simplifying the user's connectivity experience.
Kerberos Constrained Delegation	• Support for Kerberos Constrained Delegation protocol. • When a user logs into the MAG Series gateway running Junos Pulse Secure Access Service with a credential that cannot be proxied through to the backend server, the gateway will retrieve a Kerberos ticket on behalf of the user from the Active Directory infrastructure. • The ticket will be cached on the MAG Series gateway throughout the session. • When the user accesses Kerberos-protected applications, the MAG Series will use the cached Kerberos credentials to log the user into the application without prompting for a password.	• Eliminates the need for companies to manage static passwords resulting in reduced administration time and costs.
Kerberos SSO and NT LAN Manager (NTLMv2) support	• Junos Pulse Secure Access Service on MAG Series gateways will automatically authenticate remote users via Kerberos or NTLMv2 using user credentials	• Simplifies the user experience by eliminating users entering credentials multiple times to access different applications.
Password management integration	• Standards-based interface for extensive integration with password policies in directory stores (LDAP, AD, and others).	• Leverages existing servers to authenticate users. • Users can manage their passwords directly through the MAG Series gateway interface.
Web-based SSO basic authentication and NTLM	• Allows users to access other applications or resources that are protected by another access management system without reentering login credentials.	• Alleviates the need for users to enter and maintain multiple sets of credentials for web-based and Microsoft applications.
Web-based SSO forms-based, header variable-based, SAML-based	• Ability to pass user name, credentials, and other customer defined attributes to the authentication forms of other products and as header variables.	• Enhances user productivity and provides a customized experience.

Provision by Purpose

Junos Pulse Secure Access Service for the MAG Series Junos Pulse Gateways includes different access methods. These different methods are selected as part of the user's role, so the administrator can enable the appropriate access on a per-session basis, taking into account user, device, and network attributes in combination with enterprise security policies.

Table 6: Provisioning Features and Benefits

Feature	Feature Description	Benefits
Junos Pulse client	• Single, integrated, remote access client that can also provide LAN access control, and dynamic VPN features to remote users.	• Pulse replaces the need to deploy and maintain multiple, separate clients for different functionalities such as VPN and LAN access control. • The end user simply "clicks and connects."
Clientless core Web access	• Secure access to many different types of web-based applications, including many of today's most common Web applications such as Outlook Web Access, SharePoint, and many others.	• Provides the most easily accessible form of application and resource access from a variety of end user devices with extremely granular security control options. • Completely clientless approach using only a Web
IPsec/IKEv2 support for mobile devices	• Allows remote users to connect from any mobile device that supports Internet Key Exchange (IKEv2) VPN connectivity. • Administrator can enable strict certificate or username/password authentication for access via IPsec/IKEv2.	• Full L3 VPN support for new devices that support IKEv2 but for which a Junos Pulse client has not been created.
Virtual Desktop Infrastructure (VDI) support	• Allows interoperability with VMware View Manager to enable administrators to deploy virtual desktops with Junos Pulse Secure Access Service on MAG Series gateways.	• Provides remote users seamless access to their virtual desktops hosted on VMware servers. • Provides dynamic delivery of the VMware View client, including dynamic client fallback options, to allow users to easily connect to their virtual desktops.
ActiveSync Proxy	• Provides secure access connectivity (strong encryption + certificate authentication) from mobile devices (such as iOS or Android devices) to the Exchange Server via proxy, with no client software installation. • Enables up to 5,000 simultaneous sessions.	• Enables customers to allow a large number of users (including employees, contractors, and partners) to access corporate resources through mobile phones via ActiveSync.
Secure Application Manager (SAM)	• A lightweight Java or Windows-based download enabling access to client/server applications.	• Enables access to client/server applications using just a Web browser. • Also provides native access to terminal server applications without the need for a preinstalled client.
Network Connect (NC)	• Provides complete network-layer connectivity via an automatically provisioned cross-platform download, Windows Logon/Graphical Identification and Authentication (GINA) integration for domain SSO, and installer services to mitigate need for admin rights. • Allows for split tunneling capability.	• Full Layer 3 VPN tunnel with high-performance transport.

Product Options

Junos Pulse Secure Access Service currently includes several license options for enablement on the MAG Series Junos Pulse Gateways.

User License (Common Access License)

With the MAG Series Junos Pulse Gateways, common access licenses are available as user licenses. With common access licensing, the licenses can either be used for SSL VPN user sessions or UAC user sessions. (Please see the Ordering Information section below for licensing details.)

Common access user licenses provide the functionality that allows users to access the network. They fully meet the needs of both basic and complex deployments with diverse audiences and use cases, and they require little or no client software, server changes, DMZ buildouts, or software agent deployments. For administrative ease of user license counts, each license only enables as many users as specified in the license and they 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 now allow for up to 200 concurrent users.

Key features enabled by this license include:

- Junos Pulse, Secure Application Manager (SAM), and Network Connect provide cross-platform support for client/server applications using SAM, as well as full network-layer access using the SSL transport mode of Junos Pulse and the adaptive dual transport methods of Network Connect. The combination of SAM, Junos Pulse, and Network Connect with core clientless access provides secure access to virtually any audience, from remote and mobile workers to partners or customers, using a wide range of devices from any network.
- Provision by purpose goes beyond role-based access controls and allows administrators to properly, accurately, and dynamically balance security concerns with access requirements.
- Advanced PKI support includes the ability to import multiple root and intermediate certificate authorities (CAs), Online Certificate Status Protocol (OCSP), and multiple server certificates.

- User self-service provides the ability for users to create their own favorite bookmarks, including accessing their own workstations from a remote location, and even changing their passwords when they are set to expire.
- Multiple hostname support (for example, https://employees.company.com, https://partners.company.com, and https://employees.company.com/engineering) can all be made to look as though users are the only ones using the system, complete with separate logon pages and customized views that uniquely reflect the needs and desires of that audience.
- User interfaces are customizable for users and delegated administrative roles.
- Advanced endpoint security controls such as Host Checker, cache cleaner, and secure virtual workspace ensure that users are dynamically provisioned to access systems and resources only to the degree that their remote systems are compliant with the organization's security policies, after which remnant data is scrubbed from the user's device so that nothing is left behind.

High Availability Clustering Capability (No Additional License Required)

Customers have the ability to build clusters without buying any additional licenses. The clustering method can be explained in two simple steps:

1. Simply place an equal number of user ("-ADD") licenses on each box.
2. When they are joined together to form a cluster, all of the user licenses add up so that the cluster can now support all of the licensed users. For example, building a cluster of 1,000 users is done by bringing together two boxes with 500 user licenses in each of the two units.

Clustering allows you to share licenses from one MAG Series gateway with one or more additional MAG Series gateways. These are not additive to the concurrent user licenses. For example, if a customer has a 100 user license for the MAG4610 and then purchases another MAG4610, this provides a total of 100 users that are shared across both appliances, not per appliance.

Clustering supports stateful peering and failover across the LAN, so in the unlikely event that one unit fails, system configurations (such as authentication server, authorization groups, and bookmarks), user profile settings (such as user defined bookmarks and cookies), and user sessions are preserved. Failover is seamless, so there is no interruption to user/enterprise productivity, no need for users to log in again, and no downtime.

Please note that WAN clustering is not supported on the MAG Series. Multisite clustering is supported, however, provided the sites are on a campus network with LAN-like connectivity.

ICE License (Optional)

SSL VPNs can help keep organizations and businesses functioning by connecting people even during the most unpredictable circumstances—hurricanes, terrorist attacks, transportation strikes, pandemics, or virus outbreaks—the result of which could mean the quarantine or isolation of entire regions or groups of people for an extended period of time. With the right balance of risk and cost, the ICE license delivers a timely solution for addressing a dramatic peak in demand for remote access to ensure business continuity whenever a disastrous event strikes. ICE provides licenses for additional users on a MAG Series gateway running Junos Pulse Secure Access Service for a limited time.

With ICE licenses, businesses can do the following:

- Maintain productivity by enabling ubiquitous access to applications and information for employees from anywhere, at any time, and on any device
- Sustain partnerships with around-the-clock, real-time access to applications and services while knowing resources are secured and protected
- Meet federal and government mandates for contingencies and continuity of operations (COOP) compliance
- Balance risk and scalability with cost and ease of deployment

For the MAG Series, the ICE licenses are available in two forms: full ICE (which allows bursting to the full capacity of the MAG Series Junos Pulse Gateway); and a new 25% burst license (which allows bursting of up to 25% of the installed license count on any given MAG Series gateway). For example, if the customer has a MAG6610 with a 1,000 user license, the 25% burst license option will support an additional 250 users during an unplanned event.

Premier Java RDP Applet (Optional)

With the Premier Java RDP Applet option, users can remotely access centralized Windows applications independent of the client platform (Mac OS, Linux, Windows, and so on) through Java-based technology.

As a platform independent solution, the Premier Java RDP Applet lets you use the entire range of Windows applications running on the Windows Terminal Server, regardless of how the client computer is equipped. By centrally installing and managing all Windows applications, you can significantly reduce your total cost of ownership. The Premier Java RDP Applet is an OEM of the HOBlink JWT (Java Windows Terminal) product created by HOB Inc., a leading European software company specializing in Java programming.

Automatic Patch Remediation (Optional)

The Automatic Patch Remediation license combines the MAG Series secure access solutions—Junos Pulse Secure Access Service or Junos Pulse Access Control Service—with VMware's (formerly Shavlik) industry-leading asset discovery and broad update capabilities to provide an additional layer of security and control over unmanaged endpoints. The automatic patch management 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 Microsoft's System Management Server (SMS) or System Center Configuration Manager (SCCM) for remediation, and it addresses the latest operating system and software patches from Microsoft, as well as other vendors such as Adobe Systems, Mozilla Firefox, Apache, RealPlayer, and others. More information is available in the Automatic Patch Remediation License datasheet on the MAG Series webpage.

Specifications

For specification details on the MAG Series, please refer to the MAG Series Junos Pulse Gateways datasheet.

Juniper Networks Services and Support

Juniper Networks 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. Juniper Networks ensures operational excellence by optimizing the network to maintain required levels of performance, reliability, and availability. For more details, please visit **www.juniper.net/us/en/products-services**.

Ordering Information

Model Number	Description
MAG Series Junos Pulse Gateways	
MAG2600	MAG2600 Junos Pulse Gateway for SSL VPN users or UAC users. Supports up to 100 SSL VPN or 250 UAC concurrent users.
MAG4610	MAG4610 fixed configuration Junos Pulse Gateway for SSL VPN users or NAC users.
MAG6610	MAG6610 Junos Pulse Gateway for SSL VPN or NAC users; includes MAG-PS661 560 W AC power supply. Must order at least one service module (MAG-SM160 or MAG-SM360).
MAG6611	MAG6611 chassis Junos Pulse Gateway for SSL VPN or NAC users; includes MAG-PS662 750 W AC power supply. Must order at least one service module (MAG-SM160 or MAG-SM360).
Service Modules for MAG6610 or MAG6611	
MAG-SM160	MAG-SM160 service module for MAG6610 and MAG6611 gateways. Supports 1,000 SSL VPN or 5,000 UAC users.
MAG-SM360	MAG-SM360 service module for MAG6610 and MAG6611 gateways. Supports 10,000 SSL VPN or 15,000 UAC users.
MAG-CM060	MAG-CM060 management module for MAG6610 or MAG6611 gateways. Only orderable with at least one service module, and a maximum of one management module can be ordered per chassis.

Model Number	Description
User Licenses (Common Access Licenses)	
ACCESSX600-ADD-yU	Add y simultaneous users to Junos Pulse Gateway X600 Series Appliances, where y = 10 ,25, 50, 100, 250, 500, 1000, 2000, 2500, 5000, 7500, 10k, 15k, 20k, 25k
ICE Licenses	
ACCESS-ICE-25PC	In Case of Emergency (ICE) 25%: Burst to 25% of installed license count on X500 or X600 Series Appliances
MAGX600-ICE	In Case of Emergency (ICE) License for X600 Appliances
Premier RDP Applet Licenses	
ACCESS-RDP-yU-zYR	Java RDP Applet z-year subscription for y simultaneous users, where y= 50, 100, 250, 500, 1000, 2000, 2500, 5000, 7500, or 10k and z= 1, 2, or 3.
Automatic Patch Remediation Licenses	
ACCESS-PRM-yUzYR	Patch Remediation Management (PRM), z-year subscription for y simultaneous users, where y= 50, 100, 250, 500, 1000, 2000, 2500, 5000, 7500, 10K, 20K or 25K (PRM user license count cannot exceed the number of user licenses/common access licenses), and z= 1, 2 or 3

About Juniper Networks

Juniper Networks is in the business of network innovation. From devices to data centers, from consumers to cloud providers, Juniper Networks 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.juniper.net**.

Corporate and Sales Headquarters
Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or +1.408.745.2000
Fax: +1.408.745.2100
www.juniper.net

APAC and EMEA Headquarters
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
Phone: +31.0.207.125.700
Fax: +31.0.207.125.701

To purchase Juniper Networks solutions, please contact your Juniper Networks representative at +1-866-298-6428 or authorized reseller.

1000357-008-EN Nov 2013

Printed on recycled paper