SECURING TODAY'S MOBILE WORKFORCE

Connect, Protect, and Manage Mobile Devices and Users with Junos Pulse and the Junos Pulse Mobile Security Suite

Table of Contents

Executive Summary

Enterprises today are challenged with deploying mobile security and granular access control on a growing number of diverse mobile platforms, including Apple iOS, Google Android, Nokia Symbian, Microsoft Windows Mobile, and RIM BlackBerry. With increasing choices of smartphones, tablets, and other types of mobile devices, employees often bring their personal devices into the enterprise and use them to access corporate resources. This has started the trend of "Bring Your Own Device" to work (or "BYOD"), encouraging employees to use their own personal mobile devices to access the enterprise network and resources. But, BYOD carries with it issues such as mobile and network security, and it further burdens IT staff with the increasing consumerization of IT. Also, when personal mobile devices used at work are lost or stolen, enterprises risk losing sensitive corporate data such as e-mails, critical documents, or even valuable intellectual property (IP).

Juniper Networks® Junos® Pulse creates a comprehensive solution that securely connects, protects and manages enterprise mobility. The Junos Pulse solution consists of mobile device security and management provided through Juniper Networks Junos Pulse Mobile Security Suite. This is combined with secure mobile access control, which is delivered through Juniper's market-leading SSL VPN products. With this solution, enterprises can rise above the challenges of a heterogeneous mobile environment, as well as secure mobile devices from malicious attacks and theft. The richness of mobile security features in this solution, combined with a tight enforcement of access control policies as defined on the Juniper Networks MAG Series Junos Pulse Gateways running the Junos Pulse Secure Access Service, constitutes a compelling mobility solution for enterprises worldwide.

Overview

Many enterprises today struggle with the challenges involved in enabling secure, remote network and application access for mobile device users, while conforming to corporate security policies.

This paper describes how Junos Pulse and the Junos Pulse Mobile Security Suite alleviate today's enterprise mobility challenges. With a client app downloadable from leading mobile operating system application stores, Juniper's award-winning SSL VPN products, and a web-based management console, Junos Pulse and the Junos Pulse Mobile Security Suite enable enterprises to deploy security, device management, and remote access for mobile devices at scale.

Introduction

Users are beginning to use their own personal mobile devices—smartphones, tablets, and the like—to access corporate data and applications. These mobile devices are less cumbersome to carry than laptop computers, and they have the features and applications needed to deliver vital corporate data to mobile or remote users. The concept of corporate issued mobile devices is fading fast, replaced by the trend of BYOD. But enabling corporate access on personal mobile devices requires enterprises to enforce similar corporate policies, including authentication methods, data protection, access and security settings, device management, and endpoint assessment, as are already in place for their corporate managed Windows, Mac OS, and Linux based systems.

Along with the enhanced portability of mobile devices comes the risk of increased loss and theft of these devices. Enterprises risk loss of valuable, sensitive corporate data when a mobile device is lost or stolen. Users also risk loss of their personal data on lost or stolen mobile devices, since some applications are designed to store passwords, credit card numbers, bank account information, and other personal data, as well as store passwords for accessing personal apps such as social networking apps and business apps.

Finally, mobile devices run a variety of operating systems designed specifically for their smaller form factor. Most of the mobile platforms are open for third-party application development, and they support thriving application stores or marketplaces for these independently developed mobile apps. Unfortunately, this also presents a huge opportunity for hackers to build malicious applications for unsuspecting users to download. The number of threats such as viruses, trojans, and malware reported on mobile devices is increasing rapidly.

The proliferation of mobile devices presents several challenges to an enterprise:

- Adapting mobility policies to align with the current trend of employees using personal mobile devices for corporate use
- Delivering secure, remote access for mobile devices, while enforcing granular access controls
- Securing corporate and personal data, and mobile devices from malware, viruses, and malicious applications
- Mitigating the risk of loss, theft, or exploitation of corporate and personal data residing on mobile devices
- Providing all of the above for an ever increasing range of mobile devices and platforms

Junos Pulse Mobile Security Suite

Junos Pulse Mobile Security Suite is a comprehensive solution that enables enterprises to secure and manage mobile devices at scale. It protects mobile devices against malware, viruses, trojans, spyware, and other threats and malicious attacks on all of today's leading mobile platforms and operating systems. The Junos Pulse Mobile Security Suite also includes mobile device management and configuration features that mitigate the risk of losing corporate as well as personal data on lost or stolen devices; provides device configuration for accounts, policies, and application restrictions; provisions certificates; queries for, collects, and leverages device information, compliance data, and GPS position; assesses application asset management and inventory; and provides device management configuration.

The Junos Pulse Mobile Security Suite is enabled on mobile devices through Junos Pulse, which is available for the following mobile platforms in their respective application stores[1]:

- Apple iOS 4.X or later
- Google Android 2.X, 3.0 (Honeycomb), and 4.0 (Ice Cream Sandwich)
- Nokia Symbian S60 5th Edition and Symbian ^3
- Windows Mobile 6.0, 6.1, and 6.5
- BlackBerry 4.2 or later

Mobile users can download the Junos Pulse client by browsing in the "business" category of their mobile application store or marketplace.

For an administrator to configure and manage mobile security policies, the Junos Pulse Mobile Security Suite also includes the Junos Pulse Mobile Security Gateway management console. The Pulse Mobile Security Gateway is available as a hosted Software-as-a-Service (SaaS) web-based console, simplifying deployment within an enterprise, without the need to set up and maintain an onsite server. The Junos Pulse Mobile Security Gateway keeps all of the Junos Pulse Mobile Security Suite-enabled devices automatically updated with the latest emerging threat definitions, and also provides detailed reports on virus infections, updates, and the latest threats detected on mobile devices accessing the enterprise network.

Mobile Device Security on a Broad Range of Platforms

The Junos Pulse Mobile Security Suite protects mobile devices from a broad range of threats that include malware, viruses, trojans, and worms. It protects a mobile device from viruses and other malicious content that may get downloaded to the device via Short Message Service (SMS), Multimedia Messaging Service (MMS), e-mail, or other sources. It also protects the enterprise and user from data loss or unauthorized access on lost or stolen devices. One of the strengths of the Pulse Mobile Security Suite is the breadth of security features supported across most leading mobile platforms available today.

Develop Flexible Mobility Policies

Enterprises can leverage the Junos Pulse Mobile Security Suite to adapt to the current trend of employees and other authorized individuals using their personal mobile devices to access the corporate network. They can meet this challenge by not only enabling secure, granular access to corporate resources, but also by securing the user's mobile device from threats. This allows for a flexible mobility policy, enabling more employee choice while at the same time not compromising corporate security policies. The solution also enables enterprises to support a heterogeneous mobile environment spanning multiple mobile platforms.

Support the Latest Mobile Devices

The Junos Pulse Mobile Security Suite enables enterprises to support new devices and mobile operating systems as soon as they hit the market. The solution supports a broad range of operating system platforms, including Apple iOS, Google Android, Nokia Symbian, Microsoft Windows Mobile, and RIM BlackBerry. These leading mobile operating systems are powering a large majority of smartphones, tablets, and other mobile devices available worldwide. Enterprises can remain assured that by deploying the Junos Pulse Mobile Security Suite, they will be able to support new mobile devices available in the market that run any of the supported mobile platforms.

[1]The Junos Pulse for Windows Mobile client may be downloaded from **www.juniper.net/support/products/pulse/mobile/2.0/#sw**.

When employees replace their personal mobile devices with new devices, the administrator can simply de-provision the older device from the network and provision security on the newer device. The older device will then no longer be able to access the corporate network via VPN. From an enterprise perspective, this also enables a flexible model of provisioning access to new mobile devices and de-provisioning lost or stolen devices.

The Junos Pulse Mobile Security Suite antimalware service updates its virus signatures in real time over the air (OTA). The virus signatures are updated by the Juniper Networks Mobile Threat Center, Juniper's mobile malware research and analysis team. These signatures are downloaded dynamically to every mobile device running the Junos Pulse Mobile Security Suite without requiring intervention by either the user or the enterprise. This enables a low cost, real-time enforcement model for security policies on all supported devices.

Loss and Theft Protection

Enterprises can use the Junos Pulse Mobile Security Suite to retrieve lost or stolen devices by either remotely locating them via the device's GPS, or by remotely setting off alarms on them. If the device has indeed been stolen, an administrator can remotely lock the device, or even remotely wipe the device's contents through the Junos Pulse Mobile Security Gateway management console

Enterprises and users can also remotely back up the content of mobile devices and restore the backed up data to a new device when the user or enterprise replaces the lost or stolen device, regardless whether the replaced device is the same make of smartphone or tablet, or if it uses the same mobile operating system as the lost or stolen device. The loss prevention and control features of Junos Pulse Mobile Security Suite are easily administered via the web-based Junos Pulse Mobile Security Gateway management console. This gives administrators the ability and control to proactively protect the enterprise and user from losing valuable data.

Mobile Device Management (MDM)

Junos Pulse Mobile Security Suite supports MDM capabilities for most major mobile operating system platforms, enabling enterprises to set and enforce granular security and management policies on company owned and operated devices, as well as personal mobile devices used to access the enterprise network and its resources.

By supporting MDM capabilities on Apple iOS, which is the mobile operating system platform for Apple iPhones, iPads, and iPod touch devices, Junos Pulse Mobile Security Suite is easing the burden on enterprise IT staff when it comes to the growing consumerization of IT. By empowering an administrator to enable or disable certain features, to allow or disallow specific applications, and to remotely enforce security policies on a user's personal device when it is being used within the enterprise or to access the enterprise network and its applications and data, Junos Pulse Mobile Security Suite helps to ensure the enterprise's security for and from personal mobile devices and unapproved mobile apps and functions. The ability to define and enforce security policies and application restrictions protects the user, the device, the enterprise, personal and enterprise data, and intellectual property from exploit, harm, or misuse.

Junos Pulse Mobile Security Suite can also query an iPhone or IPad for specific device and compliance information, as well as enabling an inventory of apps loaded on the device. It can also capture the GPS location of an Apple iOS or Google Android device. By capturing the device's GPS location, an enterprise or employee can locate and track an employee's lost or stolen mobile device—regardless if it is a personal or corporate issued device. The device may also be remotely locked and wiped of data, particularly effective if the mobile device has been stolen for nefarious purposes.

Junos Pulse Mobile Security Suite also delivers secure device management capabilities for Google Android devices. Enterprises and service providers may set and enforce stringent passcode policies on personal or corporate-issued Android smartphones and tablets, protecting the sensitive data on the devices, as well as the corporate networks and clouds the devices are used to access. Junos Pulse Mobile Security Suite ensures that data stored and at rest on Android devices—regardless if the data is personal or business-related - is encrypted and therefore, protected.

For specific Google Android-based mobile devices, with the appropriate permissions and access rights, the Junos Pulse Mobile Security Suite can allow enterprises to automatically remove apps with no user interaction or user notification of the app's removal. Also, Junos Pulse Mobile Security Suite will automatically remove identified malware on specific manufacturers' Android mobile devices, again without user intervention or knowledge, and only with the proper permissions and rights. If an application is automatically removed from an employee's Android device, the application's removal will be noted for an administrator on the Junos Pulse Mobile Security Gateway management console. Also, Android devices from specific vendors are able to enforce encryption on data stored on their device's Secure Digital (SD) cards, in addition to data stored on the device. The MDM capabilities for Android-based devices in the Junos Pulse Mobile Security Suite are available with Android-based mobile devices from various manufacturers. Please refer to the Junos Pulse supported platforms document for further details on supported Android devices[2].

Finally, the Junos Pulse Mobile Security Suite delivers and supports several additional MDM capabilities on Google Android, Microsoft Windows Mobile, and Nokia Symbian based mobile devices. These include mobile device remote locate and track leveraging the mobile device's GPS functionality, remote device lock and wipe, SIM change notification, and other security measures related to SIM change or removal.

[2] For a list of supported devices, please refer to the Junos Pulse Supported Platforms document at **www.juniper.net/support/products/pulse/mobile**.

Granular Access Control with Juniper's SSL VPN Products

The Junos Pulse Mobile Security Suite provides a tight integration with Junos Pulse and the MAG Series Junos Pulse Gateways running Junos Pulse Secure Access Service, or the SA Series SSL VPN Virtual Appliances (or legacy SA Series SSL VPN Appliances). Junos Pulse is a single, integrated client that enables secure, mobile remote VPN access through the MAG Series gateways running Junos Pulse Secure Access Service or SA Series appliances or virtual appliances, *and* mobile device security from viruses, malware, and other threats, and device management and loss and theft protections through the Junos Pulse Mobile Security Suite.

Full Layer 3 VPN access is available via Juniper's SSL VPN solutions for Apple iOS devices, devices running Google Android 4.0, and select devices running earlier versions of Android. Full L3 VPN access via Juniper's SSL VPN platform also enables Apple iOS and select Google Android mobile devices to leverage an existing authenticated VPN session to enjoy transparent login into SAML-protected cloud- and web-based applications. It also enables iOS device users to dynamically join online meetings via Juniper Networks Junos Pulse Collaboration, which is integrated within the MAG Series gateways running Junos Pulse Secure Access Service or SA Series virtual appliances (or legacy SA Series appliances), enabling mobile users to view shared media and actively chat with other meeting attendees.

Juniper's SSL VPN platforms also enable enterprises to define security and access policies which allow, restrict ,or prohibit remote network access from any iOS and compatible Android mobile devices that are not compliant with centrally-defined enterprise corporate network security and access policies. For instance, enterprises can define a policy with Juniper's SSL VPN platform which limits remote network access to only mobile devices running specific versions of iOS or Android. Enterprises can also define an access policy preventing remote network access from jail-broken iOS devices or rooted Android devices, since jail-broken or rooted devices can pose significant security threats. An administrator can also configure the Juniper SSL VPN platforms to allow mobile, remote VPN access to network and private or public clouds from only mobile devices on which the Junos Pulse Mobile Security Suite has been activated and registered. These capabilities extend the endpoint integrity checks already offered on Juniper's SSL VPN platforms for Windows and Mac OS platforms, to iOS and Android platforms which are now used widely in corporate environments.

Enforce Strong Authentication

Junos Pulse supports strong methods of authenticating to the Juniper SSL VPN platform, including certificate-based, password-based, and multifactor authentication. Administrators can enforce the same level of authentication and access control for mobile devices and operating systems as they do for Microsoft Windows or Apple Mac OS-based systems, delivering seamless, cross-platform authentication for all users, regardless of their device.

Zero-Touch Provisioning of Mobile Access for New Users

Junos Pulse provides a simple deployment mechanism for enforcing role-based granular access control to corporate networks and applications. It is especially cost-effective when provisioning access for new employees and authorized users. New employees or authorized users need only to be instructed to download Junos Pulse from the respective, authorized application store accessible from their mobile devices, and be provided with a license code to activate Junos Pulse Mobile Security Suite features on their devices. From Junos Pulse, the appropriate policies on the MAG Series gateways running Junos Pulse Secure Access Service, or SA Series appliances or virtual appliances will provision the appropriate set of network and application access rights for the user and their device, depending on the roles and groups to which that user belongs and the assessment of their device against the enterprise's pre-defined network security and access policies.

With Junos Pulse, mobile users can become more productive from their smartphones, tablets, and other mobile devices:

- Users can access not just corporate e-mail, but also web-based applications on the corporate intranet or in the public or corporate cloud. They can also access applications such as SAP or Oracle using client applications available in the respective mobile operating platform application store.
- IT departments, meanwhile, can remain assured that managed or unmanaged, personal or corporate issued mobile devices, as well as corporate data and applications, are protected anywhere, anytime through the Junos Pulse Mobile Security Suite.

This is a unique model of provisioning access control and security for mobile devices, with seamless integration with existing VPN infrastructure. Enterprises can now establish and enforce corporate mobility policies, combining secure VPN access control and data in-transit protection with mobile security.

Junos Pulse, in conjunction with a Juniper SSL VPN platform, enables granular access control for mobile devices to the enterprise network and applications via the following methods:

- Full network access, such as access to client/server and other enterprise network- or cloud-based applications, with a similar user experience to accessing them from laptop or remote desktop PCs, for Apple iOS devices, select Google Android devices, and devices running Android 4.0

- E-mail and calendaring via ActiveSync to Microsoft Exchange servers
- Web browser-based access

Users can be dynamically provisioned with access to the corporate network and applications by one or more of the above remote access methods following policies configured on the appropriate and applicable Juniper SSL VPN platform.

Conclusion

Junos Pulse is a comprehensive solution which secures mobility—including secure mobile remote access, mobile device security and management, and application controls—protecting enterprises, their networks, clouds and data from unauthenticated, unauthorized, and insecure access, and mobile devices and the apps they access, and the data stored on-device from a wide range of threats such as viruses, malware, trojans, and worms. It provides enterprises with the security tools they need to manage a nonhomogenous mobile environment, and mitigates the risks of losing sensitive, critical corporate and personal data on lost or stolen mobile devices. These tools include the ability to remotely locate, track, wipe, and lock an employee's or other authorized user's mobile device, as well as the ability to set and manage robust device passcodes (for Apple iOS and Google Android devices), ensure stored data-at-rest is secure and set off remote alarms on a lost or stolen device. The deployment of the Junos Pulse Mobile Security Suite as a hosted SaaS offering provides the flexibility enterprises need to centrally manage all mobile security policies for their networks. The Junos Pulse Mobile Security Suite—and its Junos Pulse Mobile Security Gateway—as a hosted SaaS environment allows enterprises to quickly deploy and secure their network from insecure or ill-secured mobile devices, as well as expedite mitigation when exposed to infection and exploit.

Enterprises can also cut their overall security expenses—specifically mobile security expenses—since a SaaS solution does not require as many resources to deploy and maintain, and can support today's vast array of mobile devices needing secure access to the corporate network environment. Enterprises can enable increases to the number of secured mobile devices and users simply and quickly, while allowing the enterprise to quickly add new mobile security features and capabilities remotely over the air.

Finally, the option to seamlessly integrate the Junos Pulse Mobile Security Suite, including Junos Pulse, with the industry-leading Juniper Networks SSL VPN products—Including the MAG Series Junos Pulse Gateways running Junos Pulse Secure Access Service, or SA Series SSL VPN Virtual Appliances (or legacy SA Series SSL VPN Appliances)—provides an enterprise the required mobile endpoint assessment, and security and access features to effectively enforce corporate compliance policies. This enables enterprises to remain consistent with endpoint security and access policies that may already be in place for Microsoft Windows, Apple Mac OS and other computing platforms, thereby alleviating user confusion and potentially costly support bottlenecks.

Junos Pulse and the Junos Pulse Mobile Security Suite securely *connect, protect and manage* today's enterprise mobility.

To purchase Juniper Networks solutions, please contact your Juniper networks representative at 1-866-298-6428 or authorized reseller, or visit Juniper Networks at **www.juniper.net**.

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 408.745.2000
Fax: 408.745.2100
www.juniper.net

APAC Headquarters
Juniper Networks (Hong Kong)
26/F, Cityplaza One
1111 King's Road
Taikoo Shing, Hong Kong
Phone: 852.2332.3636
Fax: 852.2574.7803

EMEA Headquarters
Juniper Networks Ireland
Airside Business Park
Swords, County Dublin, Ireland
Phone: 35.31.8903.600
EMEA Sales: 00800.4586.4737
Fax: 35.31.8903.601

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

2000363-006-EN Aug 2012 Printed on recycled paper