MOBILE DEVICE SECURITY IN THE ENTERPRISE

Deploy secure, corporate access for mobile device users with 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 BlackBerry. With increasing choices of smartphones and other types of mobile devices, employees often bring their personal devices into the enterprise and use them to access corporate resources. When these devices are lost or stolen, enterprises risk losing sensitive corporate data such as email and documents with them.

The Juniper Networks® Junos® Pulse Mobile Security Suite creates a comprehensive solution comprising mobile device security and secure mobile access control. With this solution, enterprises can overcome the challenges of a heterogeneous mobile environment, as well as secure mobile devices from malicious attacks. The richness of mobile security features in this solution, combined with a tight enforcement of access control policies defined on the Juniper Networks SA Series SSL VPN Appliances, constitutes a compelling mobility solution for enterprises worldwide.

Introduction

Every wireless carrier in the world is reporting a rapidly increasing demand for smartphones, as compared to the earlier generation of "feature phones." Smartphones are the newest generation of devices that combine the traditional phone capabilities of feature phones with other capabilities such as availability of applications (or "apps"), bigger and higher resolution screens, more powerful processors, greater computation capacity, and expanded memory. There is also an increasingly wide range of choices in portable devices from various manufacturers, including smartphones and tablet devices.

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 the new Junos Pulse Mobile Security Suite alleviates today's enterprise mobility challenges. With the Juniper Networks Junos Pulse client application that is available from leading application stores, and a web-based management console, the Junos Pulse Mobile Security Suite enables enterprises to deploy security and remote access for mobile devices at scale.

Users are beginning to use their own, personal mobile devices to access corporate data and applications. These mobile devices are less cumbersome to carry than notebook computers or netbooks, and have the features and applications to deliver corporate data to the user. The concept of corporate-issued mobile phones is therefore beginning to fade away. But enabling corporate access on personal mobile devices requires enterprises to enforce the same corporate policies, including authentication methods, security settings, and endpoint assessment, as are already in place for their corporate managed Windows, Mac OS X, and Linux based systems.

Along with the increased portability of these 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 information, bank account information, and other personal data.

Finally, mobile devices run a variety of new 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 which attack platform vulnerabilities. The number of attacks such as viruses, trojans, and malware reported on mobile devices is steadily increasing.

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

- Adapting mobility policies to align with current trends of employees using personal mobile devices for corporate use
- Delivering secure, remote access for mobile devices, while enforcing granular access control
- 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

* Junos Pulse for Google Android and Junos Pulse for BlackBerry will be available in late October 2010. Junos Pulse for Nokia Symbian will be available in late November 2010. Junos Pulse for Windows Mobile will be available in late December 2010.

Junos Pulse Mobile Security Suite

The 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 malicious attacks on most of today's leading mobile platforms and operating systems. The Mobile Security Suite also includes mobile device management features that mitigate the risk of losing corporate as well as personal data on lost or stolen devices.

The Junos Pulse Mobile Security Suite is enforced on mobile devices through the Junos Pulse client*, which is available for the following mobile platforms in their respective application stores at no cost to users:

- Apple iOS 4.1
- Google Android* 2.0 or later
- Nokia Symbian* S60 3rd & 5th editions
- Windows Mobile* 6.0, 6.1, and 6.5
- BlackBerry* 4.2 or later

The Junos Pulse client can be downloaded by mobile device users by browsing in the "Business" category of their mobile application store or market place.

For the administrator to configure and manage mobile security policies, the Mobile Security Suite also includes the Junos Pulse Mobile Security Gateway management console. The 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 Mobile Security Gateway also provides detailed reports on virus infections, updates, and the latest threats detected on the 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 such as 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), email, or other sources. It also protects the enterprise and the user from data loss or access on lost or stolen devices. One of the strengths of the solution is the breadth of security features supported across most of the leading mobile platforms available today.

Develop Flexible Mobility Policies

Enterprises can leverage the 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 devices from threats. This allows for a flexible mobility policy, enabling more employee choice while at the same time not compromising security policies. The solution also enables enterprises to support a heterogeneous mobile environment spanning multiple mobile platforms, differing greatly from most current mobile security deployments which deem only one or two mobile platforms as being supported.

Support the Latest Mobile Devices

The Junos Pulse Mobile Security Suite enables an enterprise to support new devices and mobile operating systems as soon as they hit the market. This solution covers a broad range of operating system platforms, including Google Android, Nokia Symbian, Microsoft Windows Mobile, and RIM BlackBerry. These leading mobile operating systems are powering a large majority of all mobile devices and smartphones available worldwide. Enterprises can remain assured that by deploying the Mobile Security Suite, they can support new mobile devices available in the market, running any of these supported mobile platforms.

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 virtual private network (VPN). From an enterprise perspective, this enables a flexible model of provisioning access to new devices, and de-provisioning lost or stolen devices.

* Junos Pulse for Google Android and Junos Pulse for BlackBerry will be available in late October 2010. Junos Pulse for Nokia Symbian will be available in late November 2010. Junos Pulse for Windows Mobile will be available in late December 2010.

Deliver Real-Time Security Against Viruses and Malware

The Junos Pulse Mobile Security Suite antivirus service updates its virus signatures in real time over-the-air (OTA). The virus signatures are updated via Juniper's central Threat Management Center, by our mobile malware research and analysis team. These signatures are downloaded to every device dynamically without intervention from 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 devices by either remotely locating them via GPS, or by remotely setting off alarms on the devices. If the device has indeed been stolen, an administrator may remotely lock the device, or even remotely wipe the device's contents from the Junos Pulse Mobile Security Gateway management console.

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

Granular Access Control with the SA Series SSL VPN

The Junos Pulse Mobile Security Suite provides a tight integration with Junos Pulse and Juniper Networks SA Series SSL VPN Appliances. The security features enabled on the Junos Pulse clients can serve as an endpoint security (or Host Checker) policy on the SA Series appliances. This complements the Host Checker policies already available on the SA Series for Microsoft Windows and Apple Mac OS X platforms. The Junos Pulse client on the mobile device is a single integrated client that can provide both remote VPN access via the SA Series, as well as security from viruses, malware, and other threats through the Junos Pulse Mobile Security Suite integrated with the SA Series' Host Checker capabilities.

An administrator can configure the SA Series appliance to allow remote VPN access from only those mobile devices on which the Mobile Security Suite has been activated and registered. When the Junos Pulse Mobile Security Suite detects a virus or threat that, for some reason, cannot be quarantined and deleted, it disables the user's ability to remotely VPN to the SA Series appliance from the infected mobile device.

Enforce Strong Authentication

The Junos Pulse client supports strong methods of authenticating to the SA Series appliance, including certificate-based, password-based, and multi-factor authentication. Administrators can enforce the same level of authentication and access control for mobile devices and operating systems as from Windows or Mac OS-based systems, providing 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 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 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. Once they have done this, the policies on the SA Series appliance will provision the right set of network and application access rights for that user, depending on the roles and groups to which they belong.

Adapt to Increased Mobility

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

Users can access not just corporate email, but also web-based applications on the corporate intranet or on the corporate cloud. They can also access applications like 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 VPN access control with mobile security.

Junos Pulse, in conjunction with an SA Series appliance, enables granular access control for mobile devices to the enterprise network and applications via the following methods:

- Web (browser) based access
- Email and calendaring via ActiveSync to Microsoft Exchange servers
- Full network access, such as access to client/server and other enterprise network-based applications, similar to accessing them from notebooks, netbooks or desktop computers

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 SA Series appliance.

Conclusion

Junos Pulse Mobile Security Suite is a comprehensive mobile solution that protects mobile devices against a wide range of threats such as viruses, malware, trojans, and worms. It provides enterprises the security tools required to manage a heterogeneous mobile environment, and mitigates the risks of losing sensitive, critical corporate data on lost or stolen mobile devices. These tools include the ability to remotely locate, wipe, and lock an employee's mobile device, as well as the ability to set off remote alarms on a lost or stolen device. The deployment of the Junos Pulse Mobile Security Gateway as a hosted SaaS option provides the flexibility enterprises need to centrally manage all mobile security policies for their networks.

Finally, the option to seamlessly integrate the Junos Pulse Mobile Security Suite—including Junos Pulse—with the industry-leading SA Series SSL VPN Appliances from Juniper Networks provides enterprises the required endpoint 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 and Apple Mac OS based systems.

About Juniper Networks

Juniper Networks, Inc. is the leader in high-performance networking. Juniper offers a high-performance network infrastructure that creates a responsive and trusted environment for accelerating the deployment of services and applications over a single network. This fuels high-performance businesses. 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.

2000363-002-EN Oct 2010

Printed on recycled paper