

MAKING MOBILITY MANAGEABLE IN THE FINANCIAL SERVICES SECTOR

Safeguarding Security. Maximizing Performance. Delivering Ease of Use.

Table of Contents

Executive Summary	1
The Barriers to a High-Performance Mobile Workforce	1
Enabling the Infrastructure, Empowering Users	1
Changing the Way We Think.	2
A Question of Selection	2
Making Mobility Manageable	2
Intelligent Networking	2
Juniper Networks and Avaya	3
Ensuring Ease of Use	3
Proactive Intrusion Detection and Prevention	4
Enhancing Performance for Mobile Working	4
Conclusion	5
About Juniper Networks.	5

Table of Figures

Figure 1: Mobile working: Signing on	3
Figure 2: Mobile working: Intrusion detection and prevention integration.	4

Executive Summary

In today's marketplace, mobile working is a necessity for competitive advantage. However, the more mobile the workforce becomes, the greater the operational risk. While no company can afford to have its data communications compromised by ineffectual security or poor application performance, the penalties for financial institutions can be much greater.

If financial institutions are to maintain an advantage, they must have a network that delivers industry-leading security, access, performance and ease of use. Achieving that network means relying on more than traditional network equipment with its semi-evolved remote working functionality. It means implementing new, dynamically intelligent networking products that have been designed from the ground up to work cooperatively across the extended network. Organizations that recognize the value of mobile working—and wish to protect the advantage it provides—will actively seek such products. Those who do not will lay themselves open to higher operational risk, missed opportunities and much worse. They need high-performance networks for high-performance businesses.

This document reveals how the Juniper Networks® mobility portfolio intends to fulfill the requirement for truly mature mobile networking, delivering high-performance products that act as strategic business assets designed to enable agility and growth in the highly competitive financial services industry.

If financial institutions are to maintain an advantage, they must have a network that delivers industry-leading security, access, performance and ease of use.

The Barriers to a High-Performance Mobile Workforce

Few financial institutions now doubt the value of empowering employees to work flexibly. According to an IDC survey, as many as 69 percent now enable at least some of their sales force, personal bankers and financial advisors to access key applications and resources when away from their workstations.

Yet when poorly implemented, mobile working strategies represent a considerable risk to the financial institution—whether through the misappropriation of confidential data, the loss of business continuity, or as a result of a reduction of trust in the bank. Indeed, no organization can afford to have its data and communications compromised by a deliberate or accidental security breach, or by poor application performance.

Educating users and defining a rigorous security policy are key parts of a successful process. Moreover, the infrastructure itself has a vital role to play in enabling policy enforcement, making mobile working a safe and manageable proposition.

Accordingly, an effective mobile working strategy must be based on rock solid networking foundations.

Enabling the Infrastructure, Empowering Users

Mobile working enables employees to be more intelligent, productive and agile in the way they work, no matter where their job takes them. Unfortunately, traditional data network components are not designed to support these practices.

Many networks were created for more static ways of working, where devices were situated on-site behind both physical and electronic security perimeters. User behavior was constrained by these parameters and access to the corporate network was always maintained—invisibly to the user—through the same connection, without question of reliability, availability and network integrity.

With mobile working, traditional security perimeters no longer exist. Connection type, status and availability are key issues affecting an employee's productivity, and user behavior has become all-important to maintaining the integrity of corporate assets.

Moreover, mobile working applications increasingly include web-based applications that can create significantly more data traffic than their desktop counterparts. Add the growing trend towards voice over IP (VoIP) and other latency-sensitive applications and the result is that traditional data network components simply cannot be entrusted with mobile working.

Key Questions for Mobility

Any organization looking to implement or review a mobile working strategy should ask itself the following questions:

- How do I ensure that end-user devices do not become a point of weakness against malware and attack, particularly if we have no administrative rights to these devices?
 - How much extra cost is incurred by the need to manage software on mobile devices?
 - Will users unfamiliar with mobile working technology overload technical support resources?
 - How will users be authorized and authenticated, and how will their access be limited?
 - How will I ensure that infrastructure is future-proofed against emerging security and application requirements and user growth?
-

Changing the Way We Think

Overcoming the challenges of mobility requires the development of a well-defined mobile working strategy that understands the needs of different types of mobile workers and the areas of highest risk. But just as importantly, it involves ensuring that every element of the network is designed to provide optimal performance, security, availability and reliability.

The components of any wireless infrastructure should be selected with an understanding that security is no longer about defending a single, static barrier. Instead, it is about ensuring integrity over an extended enterprise with many dynamic perimeters.

The Juniper Networks strategy acknowledges that the majority of users are not technical experts. Access methods must be straightforward and performance assured without user involvement. Control should no longer lie at the periphery, where there is increased vulnerability to both intentional and accidental risks from end users. Financial services organizations need best-in-class networking products that shift control back onto the central infrastructure and into the hands of network administrators.

A Question of Selection

Fully mature networking technologies built on a foundation of robust, flexible and customizable solutions do exist. They deliver highly available, secure and predictable performance along with operational stability and the ease of use necessary to gain full advantage of mobile working strategies.

Making Mobility Manageable

Intelligent Networking

Meeting the demands of a mobile workforce requires components that are intelligent by design and that cooperate with other devices on the network. These are products that can make dynamic decisions for the security and performance of the infrastructure, and alleviate the burden on administrators and users alike.

Juniper Networks is a leader in creating such high-performance networking solutions. Organizations throughout the financial services sector trust Juniper Networks to lay the foundation for their mobile working programs. Juniper Networks technology delivers the transparency, control, ease of use and centralized management they need, giving companies choice and control while reducing costs.

Juniper Networks mobility portfolio consists of an advanced range of intelligent products that interact with each other to deliver:

- Secure “clientless” access to systems for ease of use
- Transparency of SSL VPN for granular role-based access
- Intrusion detection and prevention across the extended network and individual devices
- Direct control over the degree of access to resources individual users are afforded
- Reduced management responsibility through automated enforcement of policy at point of access
- SSL VPN performance to rival IPsec

Juniper Networks and Avaya

Juniper Networks and Avaya have combined industry-leading network infrastructure and applications to create end-to-end mobility solutions that address the key challenges of workforce mobility in the financial services sector. These solutions transparently extend communications and applications to mobile workers, giving every employee the same consistent set of capabilities while maintaining centralized control and management.

All Juniper Networks infrastructure products are designed to work with Avaya mobility applications and IP telephony systems. Together, Juniper Networks and Avaya deliver best-in-class solutions with proven performance and security unmatched in the industry.

Ensuring Ease of Use

For systems to remain secure, security needs to be easy to apply. Improper setup of devices and systems can harm the business. Juniper Networks SSL VPN gateway plays a key role in overcoming this failure. Enabling users to log on via a web browser, the SSL VPN is effectively clientless, making logins quick and easy and reducing time required for management and maintenance.

The gateway is also effective in simplifying the process for permissions. Because the gateway itself enforces very granular access—from authorizing which resources and applications a user can utilize, down to giving an employee read-only access to a single file—administrators can control remote user behavior in a very straightforward manner.

This level of transparency also makes it much easier for financial institutions to ensure compliance by maintaining and tracking detailed logs of user activity. Moreover, it means that providing appropriate access to guests, such as auditors or contractors, can be straightforward and well defined for each individual, alleviating the burden on network administration.

The SSL VPN gateway further ensures network security through automated functions such as Host Checker and Cache Cleaner:

- **Host Checker** assesses any device attempting to obtain access to the network, even before authentication. It performs checks for open ports and malware, levels of antivirus code and ensures that software on end devices is up-to-date and compliant. If a device is deemed unsafe, Host Checker can offer different degrees of remediation to bring the end-point back into compliance, removing the burden from the user to troubleshoot their connection.
- **Cache Cleaner** ensures that client device caches are cleaned of all controlled information when a user accesses the network from an uncontrolled device or network location, such as an Internet kiosk or Wi-Fi hot spot.

Providing appropriate access to guests, such as auditors or contractors, can be straightforward and well defined for each individual, alleviating the burden on network administration.

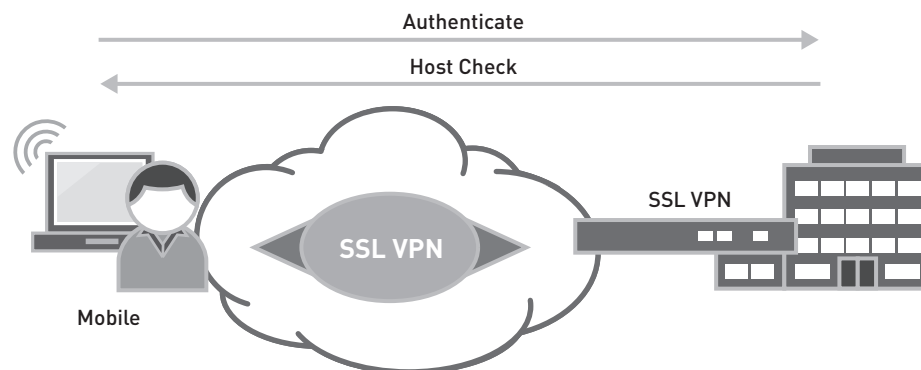


Figure 1: Mobile working: Signing on

Award Winning VPN Technology

Juniper Networks SA Series SSL VPN Appliances were one of Network World magazine's five favorite products of 2007, as voted by readers. It was previously awarded 'Best Product' in the Security Infrastructure category in 2005 and 2006.

This was the first SSL VPN appliance to gain Common Criteria Evaluation Assurance Level EAL accreditation.

Juniper Networks is also the only vendor to actively seek third party security accreditation and testing for SSL VPN appliances to ensure they meet the most stringent security requirements, both as hardened devices and secure connectivity platforms.

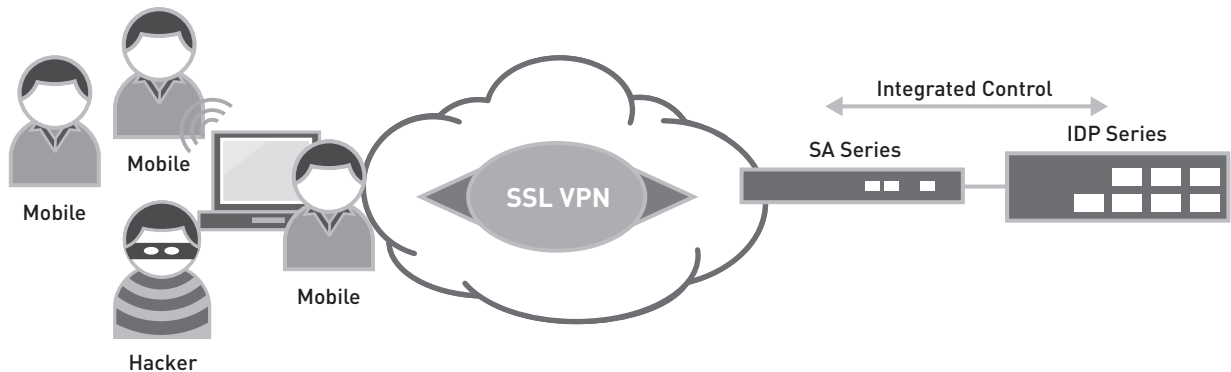


Figure 2: Mobile working: Intrusion detection and prevention integration

Proactive Intrusion Detection and Prevention

The SSL VPN gateway is designed to be cooperative with Juniper Networks IDP Series Intrusion Detection and Prevention Appliances. This means with a Juniper Networks SA Series appliance, it is possible to detect intrusions from a remote device and block access without affecting the connections of other mobile users.

Using industry leading, multi-method detection and policy-based prevention techniques, the suite enables comprehensive, easy to use protection against current and emerging threats in the mobile working environment. As a result, the suite is able to identify and stop network and application-level attacks before they inflict any damage, minimizing the time and costs associated with intrusions. This includes guarding against worms, trojans, spyware, key-loggers and other malware.

It is through interoperability with the SSL VPN gateway again that the IDP Series suite is able to enforce application usage policies for remote users. With a centralized, rule-based management approach to manage granular control over the system's behavior, this is complemented by easy access to extensive auditing and logging, as well as fully tailored reporting for compliance purposes.

Enhancing Performance for Mobile Working

Without demonstrated productivity, mobile workforces have no business case for their existence. As a result, it doesn't matter how secure the network is, or how easy the technology is to use if performance is unreliable. Increasingly, this means support for heavy web-based and latency-sensitive application traffic.

In respect of this, the Juniper Networks SSL VPN gateway rivals IPsec-based VPN systems for performance. Fully interoperable with both the SSL VPN gateway and the IDP Series suite, it provides a complete data center acceleration solution for web-enabled and IP-based business applications. The mobility portfolio is based on a unique framework, improving the end-user experience by centralizing services for server load balancing, global server load balancing, SSL encryption and termination and HTTP compression. The result is:

- Improved Web-based application performance for all users (local, remote and mobile) by up to 50 percent
- Lowered data center infrastructure and bandwidth costs by up to 60 percent
- Increased application scalability and server capacity by up to a factor of four

Conclusion

Juniper Networks is unique in the marketplace because its products interact with each other to deliver the best in mobile working security, management and control.

Organizations today recognize the role that mobility can play in their business. It is at last possible for employees to work from home or on the move with the same access to resources as in the office. Nevertheless, it is important for organizations to remember the vulnerability that this kind of empowerment creates. Addressing the underlying infrastructure is a mission-critical step, one that Juniper Networks is uniquely equipped to help financial institutions make.

Organizations that recognize the value of mobile working will put time and effort into educating users, defining a comprehensive and clear security policy and tailoring business processes to be effective.

Juniper Networks helps high-performance businesses take planned risks, innovate, and scale quickly—outpacing competitors to capture revenue, market share, and customer loyalty, even in today's hypercompetitive markets.

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.

Copyright 2010 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, Junos, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.