

ENABLE RELIABLE SECURE ACCESS FOR MOBILE USERS WITH JUNIPER NETWORKS SSL VPN

Increase Productivity for Mobile Employees, Partners, and Customers

Challenge

To remain competitive today, organizations must be able to provide network access to mobile users in order for them to stay productive and help organizations succeed.

Solution

Juniper Networks SA Series SSL VPN Appliances provides the most comprehensive support and extensive functionality to meet the demanding access needs of mobile users.

Benefits

- Increase productivity of mobile users with any time, anywhere secure network access
- Protect the network from devices that don't meet proper security credentials
- Control user access to only those resources they have authority to view
- Enable access to a broad range of users regardless of operating system or device being used
- Simplify deployment without any client software needed to install or manage

The Challenge

Mobility is a part of today's non-stop business environment. In this global economy, it's imperative that users be able to have access to corporate resources and applications regardless of where they are located, the device they are using, or what time of the day it is. Analysts agree and here's what some of them are saying.

- IDC expects the global mobile worker population to increase from 758.6 million in 2006 to more than 1 billion in 2011; this is just over 30 percent of the worldwide workforce.
- According to the most recent IDC Worldwide Mobile Worker Population Forecast, close to 75 percent of the U.S. workforce will be mobile by the end of 2011.
- Yankee Group estimates that 44 percent of all employees today are mobile workers, ranging from senior executives to entry-level sales people.

Users can no longer be tied to office environments for access to the corporate network. Just about any type of access that can be done while sitting in an office must be available while at home, at a hotel, at a customer's site, on the road, or even roaming around within the office. And users today have so many choices when it comes to communicating when they are away from the office. The array of devices include laptops, PDAs, smartphones, and kiosks to name a few. Organizations must also take into account that each device may have a different operating system (Windows, Mac OS, Linux, Symbian OS or Windows Mobile). Companies must be able to offer ubiquitous access to mobile users, at the same time making sure that access is adjusted dynamically based on the device being used, whether the device is compliant with corporate security policy, and who the user is (employee, contractor, partner, customer).

Some key business benefits of having access while being mobile include more effective use of time and greater productivity, greater responsiveness to customers and higher customer satisfaction, and greater flexibility for workers in how they do their jobs.

The Mobile Worker and a Sample Scenario

Every company defines mobile workers differently. The most basic definition is anyone who moves about in the office or in the field as opposed to staying at a fixed location like a desk. It can also be defined as workers who perform their work in multiple locations such as customer sites, company offices, homes, vendor offices, airports, and hotels. Whatever the role a mobile user plays, access to critical business information 24/7 is a necessity.

Let's examine a day in the life of a typical salesperson. He begins the day by logging in from the office using his laptop on the corporate LAN. Later he heads to the airport and needs to quickly access the company's intranet site for some information to help

him with his customer visit. But he can't use his laptop, as the airport doesn't have WiFi capability. He may want to use the kiosk or his smartphone if he has a good signal at the airport. After his customer meeting is over, he gets an order from the customer and needs to enter it quickly in his company's ordering system. In this case, he will probably use his smartphone from the customer's location. As we can see from this very typical scenario, the salesperson is truly mobile—needing access to the network quickly while being on the move, and needing flexibility to use any device that is readily available.

Today's worker often needs to multitask to ensure that other commitments and duties are staying on track. Companies must be prepared to give network access to mobile workers promptly while ensuring that each user has appropriate, devices have proper security credentials, and locations can be trusted.

The Juniper Networks Secure Access Solution for Mobile Users

Juniper Networks® SA Series SSL VPN Appliances are the ideal solution for mobile remote access because of its Web browser-based technology that enables secure access to corporate resources. IPsec VPNs, on the other hand, require an installed software client that can be resource-intensive, especially for memory constrained mobile devices, thus narrowing the variety of supported devices. With smartphone devices such as Blackberry and iPhone becoming more widely used by mobile workers, it's crucial that they have rapid access without any issues that could affect the performance of the device. SSL VPN application layer technology is also much more resilient to link fading than IPsec VPN network layer technology. This makes SSL VPN an ideal solution for securing access over mobile devices where wireless networks are often used with reduced signal strength. And because SA Series SSL VPN Appliances operate at the application level, granular access to corporate resources from mobile phones and PDAs can be audited in great detail, compared to the binary on or off access with IPsec VPNs.

With support for a wide range of mobile phones and PDA devices, SA Series SSL VPN Appliances can provide access to resources for all of your remote employees, partners, and customers worldwide, never limiting their access capabilities. Remote employees can access their email and client/server applications from anywhere and at any time with a mobile phone or PDA (if their laptop is unavailable). Partners or customers, who may have a variety of phones and PDA devices, can also easily access your applications and information when they need to help keep business moving forward.

With the SA Series' SSL VPN mobile support, your employees, partners, and customers are no longer tied to their corporate laptop or home PC. Pharmaceutical, biomedical, health care, and point of sale industries have already started to reap the productivity benefits of SSL VPN mobile device access.

The SA Series supports a comprehensive list and the latest versions of PDAs, handheld phones, and other mobile devices such as Windows Mobile, iPhone, Palm, and Symbian. The following table provides the types of mobile phone operating systems that are supported and the access methods supported by SA Series SSL VPN Appliances for respective devices. SSL VPN for remote access via mobile devices is simple to use and deploy. A single SA Series appliance can provide one management framework and user experience for all secure, remote access needs and devices—home PC, laptop, kiosk, and even mobile devices. For administrators, the SA Series makes it easy to set up and control cross-platform/cross-device access, saving time and money—unlike other expensive solutions that are known to require dedicated leased lines for just reading email. Users access applications on their mobile phone or PDA via the same URL and authentication method they use for access on other systems, saving training requirements and helpdesk support.

DEVICE		JUNIPER NETWORKS SSL VPN ACCESS METHODS AND FEATURES				
Mobile OS	Browser	Core (Web)	Email Proxy	Native ActiveSync	Application Tunneling	Endpoint Security
Windows Mobile 5	Internet Explorer	✓	✓	✓	✓	✓
Windows Mobile 6	Internet Explorer	✓	✓	✓	✓	✓
iPhone 1.x	Safari	✓	✓	N/A		
iPhone 2.x	Safari	✓	✓	✓		
Palm OS	Blazer	✓				
Symbian OS	Opera	✓		✓		
AU/KDDI	Openwave	✓		N/A	N/A	N/A
Vodafone	Openwave	✓		N/A	N/A	N/A
i-Mode	N/A	✓	N/A	N/A	N/A	N/A

ACCESS METHODS

Core (Web)	Clientless Web-based portal; provides authentication, consolidated application bookmarks, SSO to backend; full proxy
Email Proxy	POP3S/IMAPS and SMTPS Proxy, with various auth methods; Email protocols only
Native ActiveSync	Full Reverse ActiveSync Proxy, designed for use with ActiveSync; Terminates SSL, connects to backend HTTP/S service
SAM (Client/Server)	Windows software agent, delivered and installed on the fly; Tunnels specific applications, e.g. ActiveSync or MSTs
Endpoint Security	Windows software agent, delivered and installed on the fly; Ensures, for example, Symantec SmartPhone Security app is active

As part of the SA Series' market-leading "Provision by Purpose" management capability on each appliance, the solution provides unparalleled security. Robust security is ensured—whether the access point is through an internally networked PC or Web-enabled wireless mobile phone or PDA—by providing access based on the user, network access, and endpoint device being used. The SA Series supports digital certificate (x.509)-based user authentication on mobile devices and empowers the administrator to render the mobile device useless if it is stolen or lost.

SA Series SSL VPN Appliances can determine which type of device (home PC, laptop, kiosk or mobile device/PDA) is accessing the VPN by browser type, client-side certificate, and so on. End users access the same URL, regardless of the device they are using, and SA Series will dynamically determine the specific resources that an end user can access based on user, network connection, and device type. Administrators can then provision access only to those resources that are pertinent given a particular device type.

Features and Benefits

Improved Productivity and Ubiquitous Access to Network Resources

- Any time, anywhere access using any Web-enabled device to keep users productive.
- Broad cross-platform support including Windows, Mac, Linux, Symbian OS, iPhone, Windows Mobile, and others.
- Access to diverse audiences (employee, contractor, partner) using a variety of devices (corporate laptop, home PC, smartphone, kiosk) from different locations (home, airport, hotel, office).

Easy to Deploy and Manage

- Plug and play connectivity; no software to deploy, install, configure or maintain; no changes to existing servers; accessibility no matter what the platform.
- Only a Web-browser and Internet connection needed by user to simplify access experience.
- Reduces ongoing support costs versus VPN—no desktop support calls.

Greater Security

- Robust endpoint security checks to ensure that only healthy devices are granted access to network resources.
- Enables granular access control to users based on the user type, endpoint device, network connectivity location.
- Assures a healthy device is logging onto the network by determining compliance before the user is allowed access.
- Endpoint health checking to significantly reduce the influx of machines infected with viruses, trojans, and bots—even from unmanaged devices like home and contractor PCs.

Cost Savings and "Green"

- Saves money versus other remote access solutions such as IPsec VPN that require additional software and configuration.
- Lower total cost of ownership (TCO) with no software to deploy or manage.
- Reduces employee commuting costs and downtime by providing secure remote access to enterprise resources while decreasing carbon footprint.

Superior Reliability

- Proven solution deployed in tens of thousands of enterprises and service providers worldwide.
- Market-leader since SSL VPN category was created; recipient of numerous awards.

Today, the benefits extend even further with mobile access because remote users, partners, and customers are no longer tied to PCs for Internet access. Internet access is available on phones and PDAs, making it even more convenient to stay connected with a more compact device that is easy to carry virtually anywhere. SSL VPNs make an ideal solution because a simple Internet connection is all that is needed to access company applications and resources securely.

Solution Components

The Juniper Networks SA700, SA2500, SA4500, and SA6500 SSL VPN Appliances meet the needs of companies of all sizes requiring access for mobile users. SA Series appliances use SSL (Secure Sockets Layer), the security protocol found in all standard Web browsers. The use of SSL eliminates the need for pre-installed client software, changes to internal servers, and costly ongoing

maintenance and desktop support. Juniper Networks SA Series SSL VPN Appliances also offer sophisticated partner/customer extranet features that enable controlled access to differentiated users and groups without any infrastructure changes, demilitarized zone (DMZ) deployments or software agents.

The SA700 SSL VPN Appliance is specifically designed for very small enterprises as a secure, cost-effective way to deploy remote access to the corporate network. The SA2500 SSL VPN Appliance enables small- to medium-size businesses (SMBs) to deploy cost-effective remote and extranet access, as well as intranet security. The SA4500 SSL VPN Appliance is ideal for mid-to-large size organizations, while the SA6500 SSL VPN Appliance is purpose-built for large multinational enterprises and service providers.

Summary—The Most Comprehensive Secure Remote Access Solution for Mobile Users

Juniper Networks SA Series SSL VPN Appliances offer a remote access solution that addresses the flexible, 24/7 needs of mobile workers. Juniper is the market leader in SSL VPN based on market share data from leading analysts, and continues to be a leader in the Gartner Magic Quadrant. The award-winning SA Series provides the most comprehensive solution for remote access, whether mobile users are employees, partners or customers accessing applications from a laptop, home PC, kiosk, smartphone or PDA.

The bottom line is this. Today's users can simply get more done with extended access to their offices. IT organizations can rest assured that resources are secured. Access capabilities to specific applications can be defined with Juniper Networks SA Series SSL VPN Appliances based on the user, network connection, and endpoint device, including mobile phones and PDAs.

Next Steps

Please contact a Juniper Networks representative or Juniper's global network of channel partners for any questions about the SA Series SSL VPN solution.

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.



Tel North: 0151 2031400 Tel South: 0118 9071600

Email: Info@castleforce.com Web: www.castleforce.com

3510205-001-EN Feb 2009

Copyright 2009 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. "Engineered for the network ahead" and JUNOSe are trademarks of Juniper Networks, Inc. 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.



Printed on recycled paper.