

JUNOS PULSE FOR APPLE IPHONE IOS 4.1

Secure, Remote Access to Corporate Email,
Applications, and Intranet Resources via SSL VPN

Table of Contents

Introduction	3
Scope	3
Design Considerations	3
Description and Deployment Scenario	3
Junos Pulse (Layer 3 SSL VPN)	3
ActiveSync for Email, Calendar, Contacts	4
Other Secure Email Features	4
Secure Intranet and Web Applications	5
Summary	6

Introduction

The Apple iPhone offers a strong application framework for email and the Web which, when properly secured, provides instant remote access to enterprise email and intranet resources. The challenge has been providing appropriate levels of security for iPhone remote access. Enter Juniper Networks® Junos® Pulse, a new secure, remote access client that allows enterprises to provide end users with access to any type of iPhone application, while simultaneously conforming to existing enterprise security policies. Junos Pulse leverages Juniper Networks SA Series SSL VPN Appliances, which are market-leading gateways already deployed in tens of thousands of enterprises worldwide. Built for ease of use and seamless deployment, enterprises can allow their end users to be as productive on their iPhones as on their notebooks/netbooks. This, coupled with the trend for enterprise mobility and web-based applications, provides an excellent platform to help increase the efficiency of a mobile workforce.

Scope

This document covers Junos Pulse functionality now available on Apple iPhone iOS 4.1. This document also enumerates several key SSL VPN functions to further enable iPhone business applications in a secure manner.

Design Considerations

Hardware Requirements – Juniper Networks Secure Access SSL VPN Appliance

Software Requirements – Juniper Networks IVE package 7.0 and later; Apple iPhone iOS 4.1; Junos Pulse for iPhone

Description and Deployment Scenario

Junos Pulse (Layer 3 SSL VPN)

With Junos Pulse, users now have full SSL VPN access to corporate resources regardless of where they reside—in the data center, in the office, in the cloud, or at other remote sites. Junos Pulse provides a full-fledged Layer 3 VPN based on standards-based SSL encryption and authentication.

Junos Pulse offers superior performance and reliability compared to regular IPsec VPN by supporting dual transport methodologies such as high-performance Encapsulating Security Payload (ESP) transport mode, with ubiquitous SSL transport available as a fallback protocol. A myriad of authentication options are supported, including username/password, client certificate authentication, two factor/one-time password authentication (e.g., RSA SecurID), SAML, etc.

Junos Pulse also provides full support for Apple's VPN on demand, enabling seamless VPN connectivity to users via certificate authentication when accessing predefined domains. Pulse is designed to provide battery-friendly connectivity by automatically disconnecting from the VPN when the device is inactive while on Wi-Fi, reestablishing VPN connectivity when the device reactivated, and maintaining connectivity when roaming from network to network.

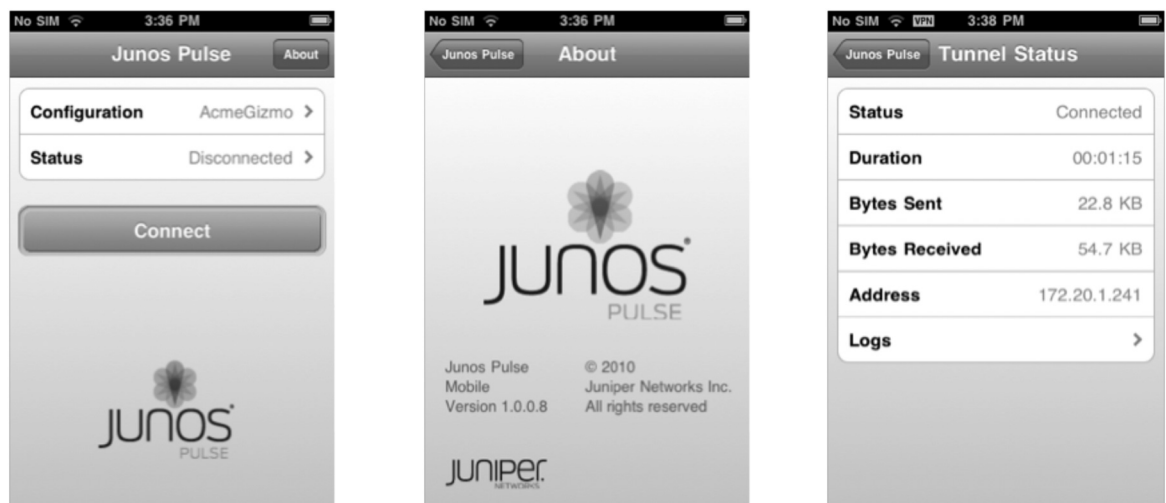


Figure 1: Junos Pulse for iPhone

ActiveSync for Email, Calendar, Contacts

With Apple iPhone 2.0+, MSFT Exchange synchronization is a snap with the over-the-air technology called Microsoft ActiveSync. This HTTP-based protocol allows the iPhone to subscribe to any changes on a user's Exchange profile, including email, calendar, and contact changes. Junos Pulse, in conjunction with SA Series SSL VPN Appliances, allows enterprise end users to synchronize their email, calendar, and contacts in a secure fashion—adding strong authentication, encryption, and a secure gateway as a termination point in the enterprise network.

Juniper Networks allows organizations to securely deploy ActiveSync in two primary ways, both of which are part of security best practices in a broader layered security approach:

Junos Pulse—This method provides Layer 3 SSL VPN connectivity so that the local email client (using ActiveSync) can talk directly over the VPN to the Exchange server(s). This solution supports a variety of native and web-based applications, including ActiveSync, VoIP applications, thin client Remote Desktop/Virtual Desktop Infrastructure (RDP/VDI), customer relationship management (CRM), database, file sharing and collaboration, Web applications using Safari, and much more.

ActiveSync Proxy—This method provides a Layer 7 HTTP proxy as a front end to the Exchange server(s). This is the simplest method in that it does not require Junos Pulse or any other VPN agent. Encryption and authentication are still available, but a user's access will be limited only to Exchange ActiveSync traffic, restricting access to additional iPhone applications.

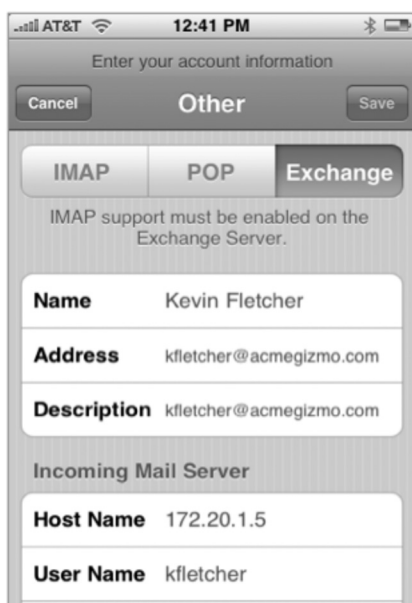


Figure 2: Exchange Settings

Securing your Exchange server/deployment with SA Series appliances and Junos Pulse provides several benefits including:

- Securing the corporate Exchange server behind a purpose-built security infrastructure, not directly accessible from the Internet
- Granular auditing and accounting records for ActiveSync and more
- Integration with existing SSL VPN authentication and authorization policies
- Full HTTP protocol inspection for additional security
- Obfuscation of internal server hostnames and IP addresses via the proxy
- Support for multiple Exchange servers in a single consolidated platform
- Enforcement for user access restrictions based on source IP, user agent, time of day, and more

Other Secure Email Features

The iPhone email system offers outbound SMTP, inbound POP3, IMAP, and Exchange/IMAP options. These services require IP-based access to the mail servers. This means corporate mail servers must be hardened and placed in a DMZ. The alternative is to protect the backend servers with a perimeter

device such as an SSL VPN. Doing so provides some additional benefits:

- **Protection**—Based on reverse proxy technology, the SSL VPN controls what data comes in, and where it can go.
- **Availability**—By making internal resources available to remote users, productivity and communications are improved.
- **Session Management**—The SSL VPN instantiates user sessions between the iPhone client and the mail servers. This helps ensure that users are properly authorized to communicate with those servers and those services. Additionally, the SSL VPN can enforce complex policies using its Dynamic Access Privilege Management framework.

Configuration of the Secure Email Proxy is rather straightforward. Users can be assigned a series of authentication options depending on specific security requirements:

- **Combined mail authentication (recommended)**—This method employs both a remote access and email password which users plug into their IMAP client configuration. The format for the IMAP password is set to ivepw,mailpw. The first of two passwords is used to authenticate users to the SSL VPN and establish their remote access session; the second password is used by the SSL VPN IMAP proxy to authenticate users to the mail service. This method provides encrypted transport and two factor authentication, and also enables the SSL VPN to securely proxy mail services.
- **Web-based email session**—This method requires users to initially log into the SSL VPN to create a special email account and password. This provides an encrypted transport and also specialized authentication credentials for mail users. Juniper recommends this method because the true mail server password is not stored on the iPhone itself.
- **Mail server authentication only**—This method links external ports 993 to the internal mail server's port 143. This provides an encrypted transport and mail server authentication only.

Secure Intranet and Web Applications

A mobile workforce such as a sales team often needs instant access to specific information (e.g., a competitive comparison between their product and another vendor's, or some data off an internal Web page). This information is commonly available only on a corporate intranet site, and rarely would that server be in a DMZ. In fact, these servers are generally deployed in a data center or other corporate infrastructure, and are only accessible externally through the use of a VPN.

The SA Series SSL VPN is built upon the Instant Virtual Extranet (IVE) platform which employs the industry's most powerful HTTPS rewriter. This rewrite function not only ensures that internal resources are accessed securely, it allows those applications to continue to work as if that Web browser were on the local network. This is because the rewriter parses and modifies HTTP and HTML content on the fly, specifically rewriting hostnames, ports, and URLs.

As a result, all subsequent "clicks" are directed to come in securely through the SA Series SSL VPN, including any data being transmitted.

In addition to securing access to intranet sites, the SA Series provides a consolidated portal with bookmarks, a robust single sign-on framework complete with Security Assertion Markup Language (SAML) federation, granular access controls, hostname obfuscation, and other advantages such as SSL acceleration and HTTP compression. These features, working together, provide streamlined secure access to resources even on the go.

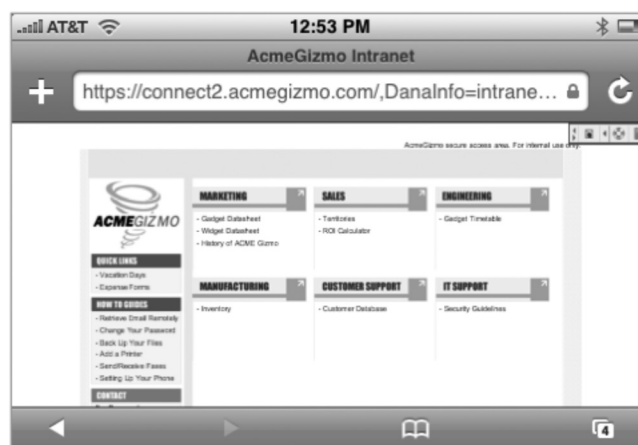


Figure 3: Secure Web Browsing

Summary

Instant access to applications, email, contacts, and the intranet are all critical elements of any successful company. Communication is key, and the iPhone enables that and so much more. The Juniper Networks SA Series SSL VPN Appliances with Junos Pulse has demonstrated support for many facets of the iPhone and other mobile devices. With deep platform support, the SA Series has become a critical foundation for securing so many technologies in so many ways. This helps keep a mobile enterprise empowered, enabled, and working more efficiently, and it is a key benefit Juniper's high-performance customers have grown to love!

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.