

# SA SERIES SSL VPN APPLIANCES



## **SA Series Leads the Market with Secure Remote Access Solutions for Organizations of Every Size**

The world's IT leaders choose Juniper Networks® SA Series SSL VPN Appliances more often because of the affordable, full featured flexibility that these solutions provide. The product family includes models sized to meet the needs of small businesses with limited IT experience, all the way up to high capacity products for large enterprises and service providers requiring the utmost authentication, authorization, and accounting (AAA) capabilities for employee, partner (extranet), and customer access.

All models use SSL transport, the secure access protocol built into every standard Web browser. SSL sessions enable any web-enabled device such as a corporate laptop, PDA, smartphone, or kiosk to securely access an organization's resources without the cost and complexity of installing, configuring, and maintaining any client software on the user device. The temporary VPN connections that SSL browsers establish also eliminate the firewall and network address translation (NAT) issues of traditional IPsec VPN products.

The SA Series includes Juniper Networks Junos® Pulse, a dynamic, integrated, multiservice network client for mobile and nonmobile devices. Junos Pulse enables optimized, accelerated, "anytime anywhere" access to corporate data. Pulse enables secure SSL access from a wide range of mobile and nonmobile devices, including smartphones, netbooks, notebooks, Wi-Fi, and 3G-enabled devices. Junos Pulse provides enterprises with improved productivity and secure ubiquitous access to corporate data and applications, anytime and from any location. For more details about Junos Pulse, please visit [www.juniper.net/us/en/products-services/software/junos-platform/junos-pulse/](http://www.juniper.net/us/en/products-services/software/junos-platform/junos-pulse/).

While almost any endpoint device is capable of accessing resources via SSL VPN, the SA Series SSL VPN Appliances can be set to enforce a number of preconditions when necessary. For example, even before a login is allowed, the SA Series appliance can be set to check the requesting device's network and device settings. This can include scanning for malware such as keystroke loggers, and verifying operation of endpoint security software such as antivirus applications and personal firewalls. The requestor's IP address, browser type, and digital certificates can also be examined before login is allowed, and the results can be used to grant or deny access based on corporate security policies.

The SA Series provides security for all enterprise tasks with options for increasingly stringent levels of access control to protect the most sensitive applications and data.

## Security, Performance, Reliability, and Management

Juniper Networks products provide best-in-class security, performance, reliability, and ease of management. These hardware accelerated platforms are performance leaders in every class, with cluster options for high availability and scalability. They feature a user interface that guides administrators to implement sweeping yet granular control over the users and groups authorized to access multiple levels of protected assets.

## Appliances with Capacities and Capabilities for Every Organization

SA Series SSL VPN Appliances span a wide range of appliances that provide small, midsize, and large enterprises, as well as service providers, with remote access plus sophisticated partner and customer extranet features. These products enable organizations to deploy differentiated access to resources based on user roles and groups. They are available with a baseline software feature set or an advanced feature set that includes options for more complex deployments.

- **SA700 SSL VPN Appliance:** targeted for small enterprises
- **SA2500 SSL VPN Appliance:** targeted for small-to-medium size enterprises
- **SA4500 SSL VPN Appliance:** targeted for mid-to-large size enterprises
- **SA6500 SSL VPN Appliance:** targeted for large enterprises and service providers
- **SSL VPN Virtual Appliance:** targeted for managed service providers offering SSL VPN to end customers

For more information on the SA Series SSL VPN Appliances, please visit [www.juniper.net/us/en/products-services/security/sa-series](http://www.juniper.net/us/en/products-services/security/sa-series).



SA700



SA2500



SA4500



SA4500 FIPS



SA6500



SA6500 FIPS

### JUNIPER NETWORKS SERVICE AND SUPPORT

Juniper Networks is the leader in performance-enabling services and support, which are designed to accelerate, extend, and optimize your high-performance network. Our services allow you to bring revenue-generating capabilities online faster so you can realize bigger productivity gains and faster rollouts of new business models and ventures. At the same time, Juniper Networks ensures operational excellence by optimizing your network to maintain required levels of performance, reliability, and availability. For more details, please visit [www.juniper.net/us/en/products-services/](http://www.juniper.net/us/en/products-services/).

FEATURES	FEATURE DESCRIPTION	BENEFITS
Cross-platform support	Ability for any platform to gain access to resources such as Windows, Mac, Linux, or various mobile devices including iPhone, Windows Mobile, Symbian, and Android.	Provides flexibility in allowing users to access corporate resources from any type of device using any type of operating system.
Junos Pulse	Single, integrated remote access client that can also provide LAN access control, WAN acceleration, and dynamic VPN features to remote users, in conjunction with Juniper Networks Unified Access Control, WXC Series Application Acceleration Platforms, and SRX Series Services Gateways	Pulse replaces the need to deploy and maintain multiple, separate clients for different functionalities such as VPN, LAN access control, and WAN acceleration. By seamlessly integrating all of these functions into one single, easy to use client, administrators can save on client management and deployment costs to end users.
Clientless core Web access	Access to web-based applications, including complex JavaScript, XML, or Flash-based applications and Java applets that require a socket connection, as well as standards-based email like Outlook Web Access (OWA), Windows, and UNIX file share, telnet/SSH hosted applications, terminal emulation, Sharepoint, and others.	Provides the most easily accessible form of application and resource access from a variety of end user machines, including handheld devices; enables extremely granular security control options; completely clientless approach using only a Web browser.
Secure Application Manager (SAM)	A lightweight Java or Windows-based download enabling access to client/server applications.	Enables access to client/server applications using just a Web browser; also provides native access to terminal server applications without the need for a preinstalled client.
Network Connect (NC)	Provides complete network-layer connectivity via an automatically provisioned, cross-platform download; Windows Logon/GINA integration for domain single sign-on (SSO); installer services to mitigate need for admin rights.	Users only need a Web browser. Network Connect transparently selects between two possible transport methods to automatically deliver the highest performance possible for every network environment. When used with Juniper Installer Services, no admin rights are needed to install, run, and upgrade Network Connect; optional standalone installation is available as well.
Host Checker	Client computers can be checked both prior to and during a session to verify an acceptable device security posture requiring installed/running endpoint security applications (antivirus, firewall, other). Also supports custom-built checks including verifying ports opened/closed, checking files/processes and validating their authenticity with Message Digest 5 (MD5) hash checksums, verifying registry settings, machine certificates, and more. Includes cache cleaner that erases all proxy downloads and temp files at logout.	Verifies/ensures that endpoint devices meet corporate security policy requirements before granting access, remediating devices, and quarantining users when necessary. Also, ensures that no potentially sensitive data is left behind on the endpoint device.
Resource authorization	Provides extremely granular access control to the URL, server, or file level for different roles of users.	Allows administrators to tailor security policies to specific groups, providing access only to essential data.
Granular auditing and logging	Can be configured to the per-user, per-resource, per-event level for security purposes as well as capacity planning.	Provides fine-grained auditing and logging capabilities in a clear, easy to understand format.
UAC-SA Federation	Seamlessly provision SA Series user sessions into Juniper Networks Unified Access Control upon login, or as an alternative, provision UAC sessions into the SA Series. Users need to authenticate only one time to get access in these types of environments.	Provides users—whether remote or local—seamless access with a single login to corporate resources that are protected by access control policies from UAC or the SA Series. Simplifies the end user experience.
High availability options	Clustering options for performance scalability to handle the most demanding usage scenarios.	Provides redundancy and seamless failover in the rare case of a system failure.
Web-based single sign-on	Allows users to access other applications or resources that are protected by another access management system without reentering login credentials.	Alleviates the need for end users to enter and maintain multiple sets of credentials for web-based and Microsoft applications.

FEATURES	FEATURE DESCRIPTION	BENEFITS
VDI (Virtual Desktop infrastructure) support	Allows interoperability with VMware View Manager and Citrix XenDesktop to enable administrators to deploy virtual desktops with SA Series appliances.	Provides seamless remote user access to virtual desktops hosted on VMware or Citrix servers. Provides dynamic delivery of the Citrix ICA client or the VMware View client, including dynamic client fallback options to allow users to easily connect to their virtual desktops.
In Case of Emergency (ICE)	Provides licenses for a large number of additional users on an SA Series SSL VPN Appliance for a limited time when a disaster or epidemic occurs.	Enables a company to continue business operations by maintaining productivity, sustaining partnerships, and delivering continued services to customers when the unexpected happens.
Anti-malware support with Enhanced Endpoint Security	Dynamically download Webroot's market-leading anti-malware software to enforce endpoint security on devices which may not be corporate assigned computers being used for network access.	Protects endpoints from infection in real time from malware and thereby protects corporate resources from harm during network access.
Juniper Networks Network and Security Manager	Intuitive centralized UI for configuring, updating, and monitoring SA Series appliances within a single device/cluster or across a global cluster deployment.	Enables companies to conveniently manage, configure, and maintain SA Series appliances and other Juniper devices from one central location.

## 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](http://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

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.

 Printed on recycled paper