

# SA SERIES SSL VPN APPLIANCES



## **Juniper Networks SA Series SSL VPN Appliances Lead the Market with Secure Remote Access Solutions That Meet the Needs of Organizations of Every Size**

The world's IT leaders choose the Juniper Networks® SA Series appliances more often thanks to the affordable, full-featured flexibility 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 requiring the utmost authentication, authorization, and auditing (AAA) capabilities for employee, partner (extranet) and customer access.

All models use secure sockets layer (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 be able to securely access an organization's resources without the cost and complexity of installing, configuring, and maintaining any client software on the device of each user. The temporary VPN connections that SSL browsers establish also eliminate the firewall and network address translation (NAT) issues of traditional IPsec VPN products.

While almost any endpoint device is capable of accessing resources via SSL VPN, the SA Series SSL VPN Appliances can be set to insist upon a number of preconditions when necessary. For example, even before a login is allowed, the appliance can be set to check the requesting device's network and device settings, including 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 provide 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 wider range of appliances that provide small, mid-size, 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



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, mobile devices.	Provides flexibility in allowing users to access corporate resources from any type of device using any type of operating system.
Antispyware support with Enhanced Endpoint Security	Dynamically download Webroot's market-leading antispyware 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 spyware and thereby protects corporate resources from harm during network access.
WX Client integration	When deployed in conjunction with the WX Client, the SA Series can dynamically provision secure, accelerated remote access for employees, partners, and contractors. For more details on the WX Client, please visit <a href="http://www.juniper.net/application-acceleration">www.juniper.net/application-acceleration</a> .	Improves end user productivity by providing LAN-like performance for accessing applications and files via Network Connect regardless of where the end user is located.
Host checker	With 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.	Scans endpoints to ensure compliance with corporate security policies both before and during the session.
Cache cleaner	All proxy downloads and temp files installed during the session are erased at logout.	Ensures that no potentially sensitive session data is left behind on the endpoint machine.
Resource Authorization	Provides extremely granular access control to the URL, server, or file level.	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 the alternative (provisioning of 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 end user experience.
Clientless core Web access	Access to Web-based applications, including complex JavaScript, XML or Flash-based apps 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 pre-installed client.
Network Connect (NC)	Provides complete network-layer connectivity via an automatically provisioned cross-platform download; Windows Logon/GINA integration for domain 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.
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 re-entering 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 the SA Series appliances.	Provides seamless access to remote users to their 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.
Multiple hostname support	Ability to host different virtual extranet Web sites from a single SA Series appliance.	Saves the cost of incremental servers, eases management overhead, and provides a transparent user experience with differentiated entry URLs.
Customizable user interface	Creation of completely customized sign-on pages.	Provides an individualized look for specified roles, streamlining the user experience.
Coordinated Threat Control	Enables SA Series SSL VPN Appliances and Juniper Networks IDP Series Intrusion Detection and Prevention Appliances to tie the session identity of the SSL VPN with the threat detection capabilities of the IDP Series, taking automatic action on users launching attacks.	Effectively identifies, stops, and remediates both network and application-level threats within remote access traffic.

## 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 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. Junos is a trademark 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