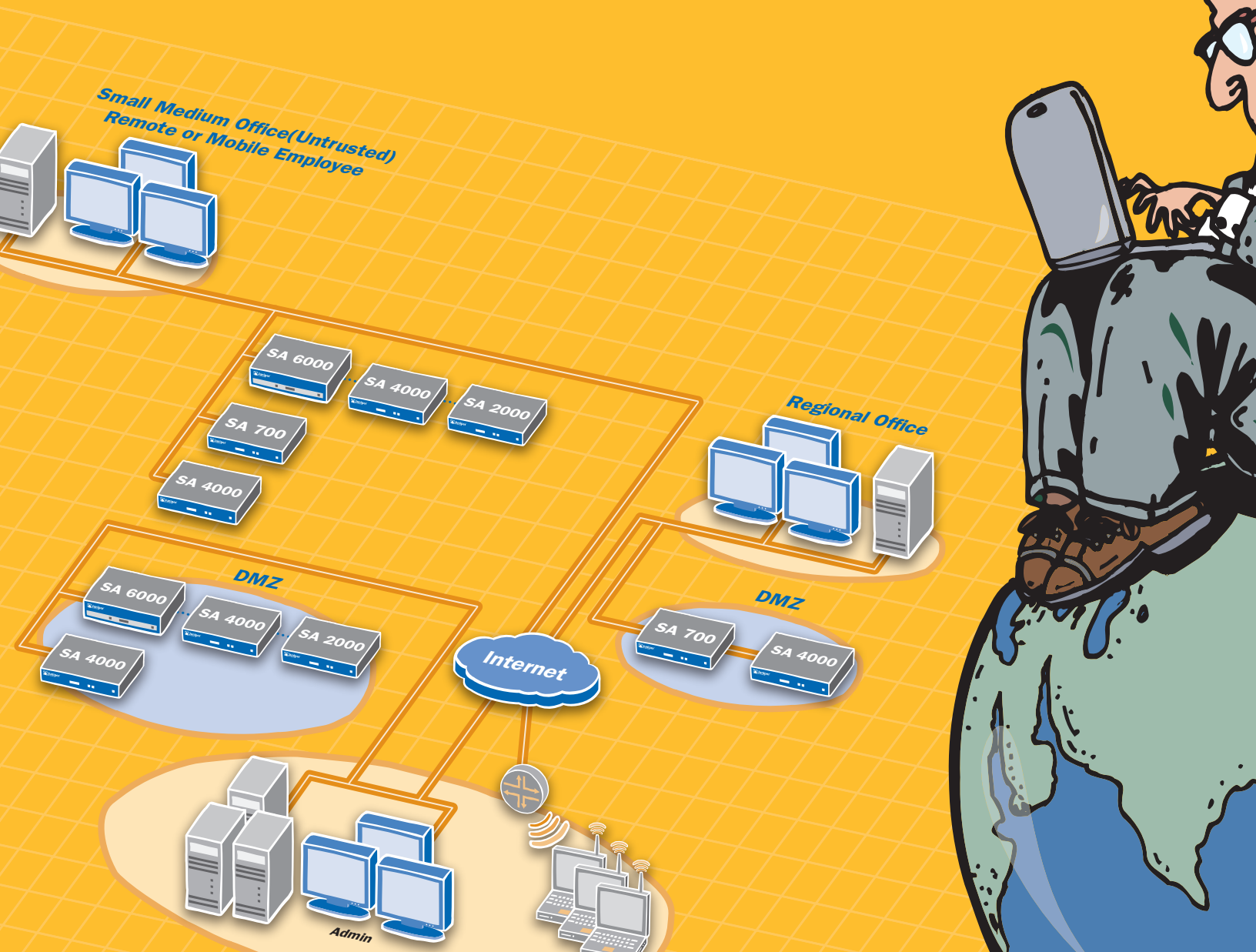


SSL VPN Solutions Portfolio

Juniper Networks Secure Access SSL VPN Appliances





Juniper Networks SA 700



Juniper Networks SA 2000



Juniper Networks SA 4000



Juniper Networks SA 4000 FIPS



Juniper Networks SA 6000/SA 6000 SP



Juniper Networks SA 6000 FIPS

Juniper Networks Secure Access 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 Juniper Networks Secure Access SSL VPN 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, 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 for 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 Juniper Networks Secure Access 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 PC'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 Juniper Networks Secure Access appliances provide security for all enterprise tasks with options for increasingly stringent levels of access control to protect the most sensitive applications and data. Secure Access appliances have been certified by leading third party security audits. The appliances are Common Criteria certified and FIPS-compliant appliances are also available.

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. Juniper backs its security and performance claims through verification by independent third party auditors, a claim unparalleled in the SSL VPN product category.

Appliances with capacities and capabilities for every organization

Juniper Networks Secure Access appliances span a wider range of appliances that provide small, mid-size, and large enterprises with remote access plus sophisticated partner/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.

Feature	Feature Description	Benefits
Cross-platform support	Ability for any platform to gain access to resources (e.g., 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
Connects using SSL	Secure connection between remote user and internal resource happens via Web connection at the application layer	Users need only a standard web browser – no special client software is required on the device
Host Checker/Cache Cleaner	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. Cache cleaner erases all proxy downloads and temp files installed during the session at logout	Scans endpoints to ensure compliance with corporate security policies both before and during the session. Cache Cleaner removes sensitive session information from the endpoint device after termination
Dynamic authentication	Enables administrators to establish a dynamic authentication policy for each unique session	Leverages the enterprise's existing investment in directories, PKI, and strong authentication
Logging and audit Capabilities	Can be configured to the per-user, per-resource, per-event level for security purposes as well as capacity planning	Facilitate security reviews and regulatory compliance in a clear, easy to understand format
Clientless Core Web access	Access to Web-based applications, including JavaScript, XML, or Flash-based apps and Java applets, as well as e-mail, Windows and UNIX file share, telnet/SSH hosted-applications, Citrix and Windows Terminal Services, Terminal Emulation, etc.	Provides the most easily accessible form of application and resource access from a variety of end-user devices, and enables granular security control options
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	Transparently selects between two possible transport methods, to automatically deliver the highest performance possible for every network environment; IPsec like 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 re-entering login credentials	Alleviates the need for end users to enter and maintain multiple sets of credentials for Web-based and Microsoft applications
Advanced Single-Sign on	Ability to pass user name, credentials, and other customer-defined attributes to the authentication forms of other products and as header variables	Enhances user productivity and provides a customized experience
Multiple Hostname support	Ability to host different virtual extranet Web sites from a single SA 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

**CORPORATE HEADQUARTERS
AND SALES HEADQUARTERS
FOR NORTH AND SOUTH AMERICA**

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

EAST COAST OFFICE

Juniper Networks, Inc.
10 Technology Park Drive
Westford, MA 01886-3146 USA
Phone: 978.589.5800
Fax: 978.589.0800

**ASIA PACIFIC REGIONAL
SALES HEADQUARTERS**

Juniper Networks (Hong Kong) Ltd.
Suite 2507-11, 25/F
ICBC Tower
Citibank Plaza, 3 Garden Road
Central, Hong Kong
Phone: 852.2332.3636
Fax: 852.2574.7803

**EUROPE, MIDDLE EAST, AFRICA
REGIONAL SALES HEADQUARTERS**

Juniper Networks (UK) Limited
Building 1
Aviator Park
Station Road
Addlestone
Surrey, KT15 2PG, U.K.
Phone: 44.(0).1372.385500
Fax: 44.(0).1372.385501

Copyright 2007 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. JUNOS and JUNOSe are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, 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.

Service and support when and where you need it

Juniper Networks Professional Services consultants and the experts of authorized Juniper Networks partners are recognized throughout the industry as knowledgeable networking specialists. They are uniquely qualified to assist you in planning and implementing a secure network.

The Customer Support Center provides responsive assistance and software upgrades, security updates, and online knowledge tools to ensure maximum reliability of Juniper Networks products. Professional instructors of Juniper Networks Educational Services help customers keep pace with rapidly evolving technologies by sharing the company's expertise on operating stable, secure networks.

To purchase Juniper Networks SSL VPN appliances, please contact your Juniper Networks sales representative or authorized reseller.

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.

