Datasheet

Juniper Networks Secure Access 6000 SP Appliance

The Juniper Networks Secure Access 6000 SP is the industry's first Secure Access SSL VPN platform with comprehensive virtualization. SA 6000 SP enables service providers (SPs) to deliver network-based SSL VPN services to multiple enterprises of any size from a single appliance/cluster. Combining Juniper Networks extensive SP expertise and its industry-leading SSL VPN feature set, the Secure Access 6000 SP gives service providers a sophisticated, end-to-end virtualization framework that is optimized for highly available and highly scalable network-based SSL VPN managed services.

Product Description

The Juniper Networks SA 6000 SP's ability to offer network-based managed services to multiple customers from a single appliance is enabled by Juniper's unique Instant Virtual System (IVS) software, which provides end customers many of the benefits of their own SSL VPN, without having to manage a device on their premises. IVS enables complete segregation of each customer's traffic, allowing SPs to securely segregate end user traffic, even if two customers have overlapping IP addresses. IVS features granular role-based VLAN (802.1Q) tagging, enabling service providers to provision specific VLANs for employees and partners of an enterprise customer. Domain Name System (DNS)/ Windows Internet Name Service (WINS), AAA, log/accounting servers, and application servers such as Web mail, file shares, and more, can reside either in the respective customers' intranets or in the SP network. SPs can provision an overall concurrent number of users on a per customer basis with the flexibility to distribute further amongst different user audiences such as remote employees, contractors, partners and others.

Architecture and Key Components

Specific SA 6000 SP hardware platform features include redundant hot swappable power supplies and hard disks with real-time data mirroring, as well as hot swappable fans. The platform also includes Gigabit Interface Connector (GBIC)-based multiple Ethernet ports with the flexibility to select SX, LX and copper-based interfaces, enabling the creation of short or long distance fiber connections and redundant or meshed configurations. Platforms can be deployed in pairs or in multi-unit clusters for High Availability (HA). The SA 6000 SP also features a state-of-the-art SSL acceleration chipset to speed CPU-intensive encrypt/decrypt processes, as well as built in compression for all traffic.

With SA 6000 SP, service providers can tailor their offerings, and they can control the degree of customer management and configuration that they wish to offer to their end customers. For example, a service provider can choose whether they wish to delegate the ability for end customers to establish their own customized user portal, endpoint security, authentication, authorization and accounting polices, or whether they would prefer to limit the offering to predefined standards.

The SA 6000 SP uses Secure Socket Layer (SSL) available in all Web browsers as a means of secure transport. This enables the service provider to offer customers a means of remote access for their mobile employees and contractors without deploying client software, as well as secure extranet or intranet access with no demilitarized zone (DMZ) buildout, server hardening, Web agent deployments or ongoing maintenance.

Features and Benefits

Low Total Cost of Ownership with High Return on Investment

The combination of the SA 6000 SP platform with IVS software allows both the service provider and the end customer to realize a wealth of benefits at a very low total cost of ownership.

- No client to install and no firewall/Network Address Translation (NAT) traversal issues result in reduced support overhead
- Differentiated revenue opportunities with services such as extranet access, business continuity, intranet LAN security and mobile device access
- Increased end customer satisfaction
- Maximizes existing SP infrastructure, including MPLS and IPSec networks

Table 1. SA 6000 SP Low Total Cost of Ownership with High Return on Investment

Feature	Feature Description	Benefit
One appliance for multiple customers	One platform to install and manage	Virtually all of the benefits of a standalone VPN, without having to manage a device on premises
Best-in-class SSL VPN features	Very rapidly growing market	Top of the line product features without requiring dedicated in-house resources
No client software to deploy, install or configure	• Very low cost • No ongoing management	• No changes to internal servers or devices • Provides access from any device (including PCs, laptops, mobile devices) with a standard Web browser
No NAT and firewall traversal issues	Reduced support overhead	Increased productivity and customer satisfaction
Extranet access with no DMZ buildout	Lucrative service requiring no changes to infrastructure	Give secure, granular access to business partners or customers with no additional infrastructure required

Complete Management Flexibility with Virtualization Framework

The granular role-based delegation features of the SA 6000 SP enable service providers to grant customer administrators a variety of management controls. Granular network, security (endpoint security, authentication, authorization and accounting), and management policies can be tailored to individual customer needs.

- Service providers can choose from a wide range of flexible options, allowing them to:
  - Delegate to end customers the ability to define the specifics of their virtual systems
  - Provide easy-to-deploy standard configurations
- Centralized management provides role-based delegation for streamlined administration

Table 2. SA 6000 SP Management Flexibility with Virtualization Framework

Feature	Feature Description	Benefit
Fully customizable look and feel at the end user level	• Can create a standard portal look and feel for quick rollout. • Can provide a differentiated offering by allowing end customers to create their own look.	• Simplify rollout to end users with a standard look. • Can give end users a familiar interface with corporate look and feel.
Configurable security features	• Can create standard security parameters for most customers to speed rollout. • Can create a differentiated offering for customers who want to leverage their own security infrastructure.	• Can use their own AAA infrastructure, or that provided by the service provider. • Can create custom AAA, endpoint security checks and remediation policies to ensure that individual security requirements are met.
Comprehensive application layer and network layer access methods with granular access controls	Can standardize offerings, or offer differentiated services with the flexibility to create customer-specific policies that reflect their own end user base needs.	• Differentiated access for a variety of end user constituencies such as employees and partners. • Each access method provides different levels of access control, from IP addresses all the way to the URL or file level.
Auditing and logging	• SPs can offer auditing and logging services or end customers can use their own log/accounting servers. • With log data, SPs can help end customers with regulatory compliance. • Customer-specific RADIUS accounting facilitates seamless billing integration with existing billing applications.	• Log data can be replicated to the customer's log servers. • SP services aid with regulatory compliance without requiring in-house expertise. • Verify billing data.

Best-in-Class End User Features that Customers Demand

- A variety of value-added access methods, so that customers can provision by purpose
- End-to-end layered security

Service Provider Performance, Scalability and High Availability

The SA 6000 SP features a number of benefits to meet service provider performance, scalability and HA needs, including:

- Redundant, hot swappable components
- A variety of performance enhancing features including hardware-based SSL acceleration, compression and clustering for optimal scalability and availability
- Multi-unit cluster deployment option, for HA across the LAN and the WAN

Table 3. Service Provider Performance, Scalability and High Availability

Feature	Service Provider Benefits
Hardware-based SSL acceleration	Offloads compute-intensive encrypt/decrypt process from the CPU, enhancing performance
Built-in compression for all traffic	Faster application performance and response times for all traffic traversing the IVE such as HTTP, file, and client/server application traffic
Clustering and stateful peering	• Cluster pairs or multi-unit clusters deployed across the LAN or across the WAN for superlative scalability with a large number of user licenses, which scales access as the user base grows • Units that are part of a cluster that synchronizes system-state, user profile-state and session-state data among a group of appliances in the cluster for seamless failover with minimal user downtime and loss of productivity
Dual redundant hot swappable power supplies and hard disks with real time data mirroring **Hot swappable fans**	• Ensures HA and high reliability with component level redundancy and data mirroring in hard disk • Optimized uptime with hot swappable components resulting in operational convenience in the rare event of failure of a component
GBIC-based ports with flexibility to select SX, LX and copper-based GBIC interfaces	Fully redundant/meshed configuration of SSL VPN appliances with multiple load balancers for optimized uptime
Dual Gigabit Ethernet interfaces	Enables strong performance in the highest speed enterprise networks

Streamlined Service Provider Administration

The SA 6000 SP provides streamlined administration to most efficiently provision multiple customers. It also features standards-based management protocols to facilitate integration with third-party management and reporting products.

Table 4. Streamlined Service Provider Administration

Feature	Service Provider Benefits
Centralized management	Unified cluster management with synchronized push configuration, zero downtime upgrade, backup configuration and restore, dynamic log filtering and deterministic cluster recovery
Out of band management port	Allows management via an interface segregated from user traffic
Binary and XML configuration import/export	• Platform configuration that can be exported and imported for streamlined multi-box configuration • XML export/import that can be leveraged for an application programming interface (API) to the provisioning system • Easily accessible XML configuration data that aids with regulatory compliance
SNMP	• Real-time system health monitoring with SNMP MIBs for critical parameters such as CPU and memory utilization, concurrent number of users and more • Customer-specific maintenance and troubleshooting with virtualized SNMP traps for major and critical events
Troubleshooting and diagnostics	Virtualized troubleshooting and diagnostics that enable SPs to service individual customers without affecting other customers hosted on the same system

Best-in-Class SSL VPN Features that End Users Demand

Juniper Networks market-leading Secure Access SSL VPN offerings provide an unmatched feature set. These features are available to end customers as part of a virtualized system, allowing the service provider to choose to offer them as part of a standard or differentiated service offering. More detailed information on the standard Juniper Networks SA SSL VPN features can be found in the Secure Access family datasheets.

Table 5. Best-in-Class SSL VPN Features

Feature	Feature Description	Benefit
Access privilege management capabilities	• Hybrid role-/resource-based policy model • Pre-authentication assessment • Dynamic authentication policy • Dynamic role mapping • Resource authorization • Granular auditing and logging • Extensive directory integration and broad interoperability	Ensures dynamic, granular access based on the user type, health of the endpoint device, and the network connectivity location of the user
Provision by purpose	• **Clientless Core Web**—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. • **Secure Application Manager (SAM)**—A lightweight Java or Windows-based download 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**—Provides complete network-layer connectivity via an automatically provisioned, cross platform download from a Web browser. Adaptive dual mode transport for optimal network layer connectivity in diverse connection environments.	Provides three flexible, distinct methods to control users' access to resources
End-to-end layered security	• Native Host Checker • Host Checker API • Host Check Server Integration API • Policy-based enforcement and remediation • Secure Virtual Workspace • Cache Cleaner • Integrated malware protection • Coordinated threat control	Extensive end-point security checks before and during the session to protect the corporate network
User self-service features	• Password management integration • Web-based single sign-on • BASIC Auth and NTLM, forms-based, header variable-based	Comprehensive password management features to simplify administration for the IT department

Product Options

Upgrade Options

Hardware

- Replacement hot swappable chassis fan
- Small form factor pluggable (SFP) transceiver
  - 1000BASE-T RJ45 copper
  - 1000BASE-SX fiber
  - 1000BASE-LX fiber

Software

- Instant Virtual System (IVS) upgrade option
- Secure Application Manager and Network Connect upgrade option (SAMNC)
- Advanced Software Feature set (includes Central Manager)
- Secure Meeting upgrade option

Specifications

SA 6000

- Dimensions (W x H x D): 16.7 x 3.5 x 16.2 in (42.42 x 8.89 x 41.15 cm)
- Weight: 28.5 lb (12.94 kg) typical (unboxed)
- Material: 18 gauge (.048 in) cold-rolled steel
- Fans: 2 externally accessible, hot swappable ball-bearing fans
- 19 in rack-mountable

Panel Display

- Front panel power button
- Power LED, HD activity, temp, PS fail
- Hard disk drive (HDD) Activity and Redundant Array of Independent Disks (RAID) status LEDs

Ports

Network

- Traffic
  - Two RJ-45 Ethernet: 10/100/1000 full or half-duplex (auto-negotiation)
  - Two SFP ports: Gig-E
- Fast Ethernet: IEEE 802.3u compliant
- Gigabit Ethernet: IEEE 802.3z or IEEE 802.3ab compliant

Console

- Management: One RJ-45 Ethernet, 10/100/1000 full or half-duplex (auto-negotiation)
- One 9-pin serial console port

Power

- AC Power Wattage: 500 W
- AC Power Voltage: 100-240 V AC, 50-60 Hz, 5 A Max
- System Battery: CR2032 3V lithium coin cell
- Efficiency: 65% minimum, at full load
- Mean time between failures (MTBF): 78,000 hours

Environmental

- Operating temperature: 50° to 104° F (10° to 40° C)
- Storage temperature: -40° to 158° F (-40° to 70° C)
- Relative humidity (operating): 8 to 90% noncondensing
- Relative humidity (storage): 5 to 95% noncondensing
- Altitude (operating): -50 to 10,000 ft (3,000 m)
- Altitude (storage): -50 to 35,000 ft (10,600 m)

Safety and Emissions Certification

- Safety: EN60950-1:2001 + A11, UL60950-1:2003, CSA C22.2 No. 60950-1, IEC 60950-1:2001
- Emissions: FCC Class A, VCCI Class A, CE Class A

Warranty

- 90 days—can be extended with support contract

Safety and Emissions Certification

- Common criteria certified
- Federal Information Processing Standards (FIPS) appliances available

Ordering Information

Model Number	Description
Secure Access 6000 Base System	
SA6000SP	Secure Access 6000 Base System Service Provider Series
Secure Access 6000 User Licenses	
SA6000-ADD-100U	Add 100 simultaneous users to SA 6000
SA6000-ADD-250U	Add 250 simultaneous users to SA 6000
SA6000-ADD-500U	Add 500 simultaneous users to SA 6000
SA6000-ADD-1000U	Add 1000 simultaneous users to SA 6000
SA6000-ADD-2500U	Add 2500 simultaneous users to SA 6000
SA6000-ADD-5000U	Add 5000 simultaneous users to SA 6000
SA6000-ADD-7500U*	Add 7500 simultaneous users to SA 6000
SA6000-ADD-10000U*	Add 10000 simultaneous users to SA 6000
SA6000-ADD-12500U*	Add 12500 simultaneous users to SA 6000
SA6000-ADD-15000U*	Add 15000 simultaneous users to SA 6000
*Multiple SA6000's required	
Secure Access 6000 Feature Licenses	
SA6000-ADV	Advanced for SA 6000
SA6000-IVS	Instant Virtual Systems for SA 6000
SA6000-SAMNC	Secure Application Manager and Network Connect for SA 6000
SA6000-MTG	Secure Meeting for SA 6000
Secure Access 6000 Clustering Licenses	
SA6000-CL-100U	Clustering: Allow 100 users to be shared from another SA 6000
SA6000-CL-250U	Clustering: Allow 250 users to be shared from another SA 6000
SA6000-CL-500U	Clustering: Allow 500 users to be shared from another SA 6000
SA6000-CL-1000U	Clustering: Allow 1000 users to be shared from another SA 6000

Model Number	Description
Secure Access 6000 Clustering Licenses cont'd	
SA6000-CL-2500U	Clustering: Allow 2500 users to be shared from another SA 6000
SA6000-CL-5000U	Clustering: Allow 5000 users to be shared from another SA 6000
SA6000-CL-7500U	Clustering: Allow 7500 users to be shared from another SA 6000
SA6000-CL-10000U	Clustering: Allow 10000 users to be shared from another SA 6000
SA6000-CL-12500U	Clustering: Allow 12500 users to be shared from another SA 6000
SA6000-CL-15000U	Clustering: Allow 15000 users to be shared from another SA 6000
Accessories	
SA6000-PS	Field Upgradeable Secondary Power Supply for SA 6000
SA6000-HD	Field Upgradeable Secondary Hard Disk for SA 6000
SA6000-MEM	Field Upgradeable (by authorized VAR only) Additional 2 GB Memory for SA 6000
SA6000-FAN	Field Replaceable Fan for SA 6000
SA-ACC-RCKMT-KIT-2U	Spare Secure Access Rack Mount Kit - 2U
SA-ACC-PWR-AC-USA	Spare Secure Access AC Power Cord USA
SA-ACC-PWR-AC-UK	Spare Secure Access AC Power Cord UK
SA-ACC-PWR-AC-EUR	Spare Secure Access AC Power Cord EUR
SA-ACC-PWR-AC-JPN	Spare Secure Access AC Power Cord JPN
SA6000-GBIC-FSX	GBIC Transceiver—Fiber SX for SA6000
SA6000-GBIC-FLX	GBIC Transceiver—Fiber LX for SA6000
SA6000-GBIC-COP	GBIC Transceiver—Copper for SA6000

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.

Juniper NETWORKS

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

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

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.
26/F, Cityplaza One
1111 King's Road
Taikoo Shing, Hong Kong
Phone: 852.2332.3636
Fax: 852.2574.7803

100134-007 June 2008

To purchase Juniper Networks solutions, please contact your Juniper Networks sales representative at 1-866-298-6428 or authorized reseller.