



Juniper Networks Secure Access 2000, 4000, and 6000 Appliances

Juniper Networks Secure Access products lead the SSL virtual private network (VPN) market with a complete range of remote access appliances, including the Secure Access 2000 (SA 2000), Secure Access 4000 (SA 4000), and Secure Access (SA 6000). Juniper Networks Secure Access appliances combine the security of SSL with standards-based access controls, granular policy creation, and unparalleled flexibility. The result provides ubiquitous security for all enterprise tasks with options for increasingly stringent levels of access control to protect the most sensitive applications and data. Juniper Networks Secure Access appliances deliver lower total cost of ownership over traditional IPSec client solutions and unique end-to-end security features.

Product Description

The Juniper Networks SA 2000, SA 4000, and SA 6000 SSL VPN appliances meet the needs of companies of all sizes. Secure Access appliances are based on the Instant Virtual Extranet (IVE) platform, which uses SSL, the security protocol found in all standard Web browsers. The use of SSL eliminates the need for pre-installed client software deployment, changes to internal servers, and costly ongoing maintenance and desktop support. Juniper's Secure Access appliances also offer sophisticated partner/customer extranet features that enable controlled access to differentiated users and groups with no infrastructure changes, no DMZ deployments, and no software agents.

Architecture and Key Components

The Juniper Networks SA 2000 SSL VPN enables small- to medium-size businesses (SMBs) to deploy cost-effective remote and extranet access, as well as intranet security. Users can access the corporate network and applications from any machine over the Web. The SA 2000 offers High Availability (HA) with seamless user failover.

The Juniper Networks SA 4000 SSL VPN enables mid-to-large size organizations to provide cost effective remote employee and partner extranet access using only a Web browser. The SA 4000 appliances feature rich access privilege management functionality that can be used to create secure customer/partner extranets. This functionality also allows the enterprise to secure access to the corporate intranet, so that different employee and visitor populations can utilize exactly the resources that they need while adhering to enterprise security policies. Built-in compression for all traffic types speeds performance, and hardware-based SSL acceleration is available for more demanding environments. The SA 4000 also offers High-Availability (HA) with seamless user failover.

The Juniper Networks SA 6000 SSL VPN is purpose-built for large enterprises and service providers. It features best-in-class performance, scalability, and redundancy for organizations with high volume secure access and authorization requirements. Additionally, the SA 6000 offers High Availability (HA) with seamless user failover. The SA 6000 hardware platform, complete with multi-unit clustering options, is designed to scale to the largest enterprise deployments, with available redundant hot swappable hard disks, power supplies, and fans, as well as GBIC-based multiple Ethernet ports for redundant or meshed configurations. The SA 6000 also features a built-in compression for web and files, and a state-of-the-art SSL acceleration chipset to speed CPU-intensive encrypt/decrypt processes.

Features and Benefits

High-scalability Support on Secure Access 6000 SSL VPN

The SA 6000 is designed to meet the growing needs of large enterprises and service providers with its ability to support thousands of users accessing the network remotely. The following table shows the number of concurrent users that can be supported on the SA 6000 platform:

- Single SA 6000: Supports up to 5,000 concurrent users
- Two-unit cluster of SA 6000s: Supports up to 8,000 concurrent users
- Three-unit cluster of SA 6000s: Supports up to 12,000 concurrent users
- Four-unit cluster of SA 6000s: Supports up to 15,000 concurrent users

All performance testing is done based on real-world scenarios with simulation of traffic based on observed customer networks. In the case of Core Access, this means real web applications are being accessed, which entails rigorous HTML rewriting and policy evaluation.

End-to-End Layered Security

The SA 2000, SA 4000, and SA 6000 provide complete end-to-end layered security, including endpoint client, device, data, and server layered security controls.

These include:

Feature	Feature Description	Benefit
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, etc.) 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	Verifies/ensures that endpoint device meets corporate security policy requirements before granting access, remediating devices and quarantining users when necessary
Host Checker Application Programming Interface (API)	Created in partnership with best-in-class endpoint security vendors. Enables enterprises to enforce an endpoint trust policy for managed PCs that have personal firewall, antivirus clients, or other installed security clients, and quarantine non-compliant devices	Utilize current security policies with remote users and devices; easier management
Trusted Network Connect (TNC) Support on Host Checker	Allows interoperability with diverse endpoint security solutions from antivirus to patch management to compliance management solutions	Enables customers to leverage existing investments endpoint security solutions from third-party vendors
Policy-based Enforcement	Allows the enterprise to establish trustworthiness of non-API compliant hosts without writing custom API implementations or locking out external users, such as customers or partners that run other security clients	Enables access to extranet endpoint devices like PCs from partners that may run different security clients than that of the enterprise
Hardened security appliance and Web server	Hardened security infrastructure extensively audited by third-party security experts including CyberTrust, iSec Partners, and has also received Common Criteria Certification	Not designed to run any additional services and is thus less susceptible to attacks; no backdoors to exploit or hack
Security Services Employ Kernel-level Packet Filtering and Safe Routing	Undesirable traffic is dropped before it is processed by the TCP stack	Ensures that unauthenticated connection attempts, such as malformed packets or denial of service (DOS) attacks, are filtered out
Secure Virtual Workspace (Advanced Feature Set)	A secure and separate environment for remote sessions that encrypts all data and controls I/O access (printers, drives, etc.)	Ensures that all corporate data is securely deleted from a kiosk or other unmanaged endpoint after a 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
Data Trap and Cache Controls	Rendering of content in non-cacheable format	Prevents sensitive metadata (cookies, headers, form entries, etc.) from leaving the network
Integrated Malware Protection	Pre-installed checks to protect users & devices from keyloggers, trojans, and remote control applications	Enables customers to provision endpoint containment capabilities
Coordinated Threat Control	Enables Juniper's SA SSL VPN and intrusion detection and prevention (IDP) appliances to tie the session identity of the SSL VPN with the threat detection capabilities of IDP, taking automatic action on users launching attacks	Effectively identify, stop, and remediate both network and application-level threats within remote access traffic

Lower Total Cost of Ownership

In addition to enterprise-class security benefits, the SA 2000, SA 4000, and SA 6000 have a wealth of features that enable low total cost of ownership.

Feature	Feature Description	Benefit
Uses SSL	Secure connection between remote user and internal resource is via a Web connection at the application layer	Secure remote access with no client software deployment, maintenance, and no changes to existing servers; no firewall proxy and network address translation (NAT) traversal issues
Based On Industry-standard Protocols and Security Methods	No installation or deployment of proprietary protocols required	The investment in the SA appliance can be leveraged across many applications and resources over time
Extensive Directory Integration and Broad Interoperability	Existing directories in customer networks can be leveraged for authentication and authorization enabling granular secure access without recreating those policies	Existing directory investments can be leveraged with no infrastructure changes; no API's for directory integration as it's all native/built in
Integration with Strong Authentication and Identity and Access Management Platforms	Ability to support SecurID, SAML, PKI/digital certificates	Leverages existing corporate authentication methods to simplify administration
Multiple Hostname Support (Advanced Software Feature Set)	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 (Advanced Software Feature Set)	Creation of completely customized sign-on pages	Provides an individualized look for specified roles, streamlining the user experience
Juniper Networks Central Manager (Advanced Software Feature Set)	Intuitive Web-based UI for configuring, updating, and monitoring SA appliances within a single device/cluster or across a global cluster deployment	Conveniently manage, configure, and maintain SA appliances from one central location
"In Case of Emergency" (ICE)	Provides licenses for a large number of additional users on a SA 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
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

Rich Access Privilege Management Capabilities

The SA 2000, SA 4000, and SA 6000 provide dynamic access privilege management capabilities without infrastructure changes, custom development, or software deployment/maintenance. This facilitates the easy deployment and maintenance of secure remote access, as well as secure extranets and intranets. When a user logs in to the SA appliance, they pass through a pre-authentication assessment, and are then dynamically mapped to the session role that combines established network, device, identity, and session policy settings. Granular resource authorization policies further ensure exact compliance to security strictures.

Feature	Feature Description	Benefit
Hybrid Role-/Resource-based Policy Model	Administrators can tailor access	Ensures that security policies reflect changing business requirements
Pre-authentication Assessment	Network and device attributes, including presence of Host Checker/Cache Cleaner, results of endpoint security scans, source IP, browser type, and digital certificates, can be examined before login is allowed	Results used in dynamic policy enforcement decisions
Dynamic Authentication Policy	Enables administrators to establish a dynamic authentication policy for each unique session	Leverages the enterprise's existing investment in directories, PKI, and strong authentication
Dynamic Role Mapping	Combines network, device, and session attributes to determine which of three different types of access is allowed	Enables the administrator to provision by purpose for each unique session
Resource Authorization	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	Fine-grained auditing and logging capabilities in a clear, easy to understand format
Custom Expressions (Advanced Software Feature Set)	Enables the dynamic combination of attributes on a "per-session" basis, at the role definition/mapping rules and the resource authorization policy level	Finer granularity and customization of policy roles

User Self-Service

The SA 2000, SA 4000, and SA 6000 offer comprehensive password management features. These features increase end user productivity, greatly simplify administration of large diverse user resources, and significantly reduce the number of help desk calls.

Feature	Feature Description	Benefit
Password Management Integration	Standards-based interface for extensive integration with password policies in directory stores (LDAP, Microsoft Active Directory, NT, etc.)	Leverage existing servers to authenticate users; users can manage their passwords directly through the SA interface
Web-based Single Sign-On (SSO) Basic Authentication and NTLM	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
Web-based SSO Forms-based, Header Variable-based, SAML-based (Advanced Feature Set)	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

Provision by Purpose

The SA 2000, SA 4000 and SA 6000 include three different access methods. These different methods are selected as part of the user's role, so the administrator can enable the appropriate access on a per-session basis, taking into account user, device, and network attributes in combination with enterprise security policies.

Feature	Feature Description	Benefit
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 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 machines, including handheld devices, and enables extremely granular security control options. Completely clientless approach using only a web browser
Secure Application Manager (SAM) (SAMNC License)	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) (SAMNC License)	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 need only 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 needed to install, run, and upgrade Network Connect; optional stand-alone installation available as well

Product Options

The SA 2000, SA 4000, and SA 6000 have several hardware and software options that can be added to the products.

Advanced Endpoint Defense: Integrated Malware Protection Option

Advanced Endpoint Defense: Malware Protection is an endpoint security software module that integrates with Host Checker and provides protection from unwanted malware, such as trojan horses and key loggers residing on an endpoint from which an end user is looking to start a remote access session. The malware module is configured as a Host Checker module and is dynamically delivered to the end-user's PC, with no software to pre-install. All Secure Access appliances include a license for 25 concurrent users, free of charge. Customers must purchase additional licenses in order to increase this functionality to support more users.

The Advanced Endpoint Defense: Integrated Malware Protection upgrade is available for the SA 2000, SA 4000, and SA 6000.

Secure Application Manager and Network Connect Upgrade Option

The SAM and NC upgrade is a companion to Juniper Networks Core Clientless access for SSL VPNs. SAM and NC provide cross-platform support for client/server applications using SAM, as well as full network-layer access using the adaptive dual transport methods found in NC. The combination of SAM and NC with Core Clientless access will provide secure access to virtually any audience, from remote/mobile workers to partners or customers, using a wide range of devices from any network. Although SAM and NC deliver two different access methods, administrators can specify exactly which access method, or combination of access methods, they wish to assign for each user in every deployment scenario. This allows administrators to provision by purpose, balancing security concerns with access requirements. Dynamic access controls enable the access to change as user, endpoint, and network criteria change.

The SAMNC upgrade is available for the SA 2000, SA 4000, and SA 6000.

Advanced Feature Set

The Secure Access appliances are offered with either Baseline or Advanced feature sets, designed to create an affordable solution that meets the needs of every company, from SMB employee remote access deployments to the largest global enterprise extranet. The Baseline features that come with the appliance provide the functionality that an enterprise would need to deploy secure remote access, as well as a provision a basic customer/partner extranet or intranet. The Advanced feature set provides additional sophisticated capabilities that will meet the needs of more complex deployments with diverse audiences and use cases, including Secure Access Central Manager, a robust product with an intuitive Web-based UI designed to facilitate the task of configuring, updating, and monitoring a single Secure Access appliance or a single cluster deployment. Both feature sets provide remote access, extranet, and intranet capabilities with little to no need for client software, server changes, DMZ build-outs, or software agent deployments. The Advanced feature set includes:

- Advanced PKI support including ability to import multiple root and intermediate CAs, OCSP, and multiple server certificates
- User self service
- Access Management Integration
- Multiple hostname support
- Customizable UI
- Combine attributes using Boolean expressions, for flexible, dynamic, “per-session” policies
- Advanced role definition and role mapping rules combine attributes using Boolean expressions
- Advanced resource authorization policies combine attributes using Boolean expressions
- Role-based delegation, configurable at the individual task level
- Flexible role definition
- Juniper Networks Central Manager
- Secure Virtual Workspace

The Advanced Feature upgrade is available for the SA 2000, SA 4000, and SA 6000.

Secure Meeting Option

The Secure Meeting upgrade license extends the capabilities of the Juniper Networks Secure Access appliances by providing secure anytime, anywhere, cost effective online Web conferencing and remote control PC access. Secure Meeting enables real-time application sharing so authorized employees and partners can easily schedule online meetings or activate instant meetings through an intuitive Web interface that requires no training or special deployments. Help desk staff or customer service representatives can provide remote assistance to any user or customer by remotely controlling their PC without requiring the user to install any software. Best-in-class authentication, authorization, and accounting (AAA) capabilities enable companies to easily integrate Secure Meeting with their existing internal

authentication infrastructure and policies. Juniper’s market-leading, hardened, and Common Criteria certified SSL VPN appliance architecture and SSL/HTTPS transport security for all traffic means that administrators can rest assured that their Web conferencing and remote control solution adheres to the highest levels of enterprise security requirements.

The Secure Meeting upgrade is available for the SA 2000, SA 4000, and SA 6000.

Instant Virtual System Option

Juniper Networks Instant Virtual System (IVS) option is designed to enable administrators to provision 255 logically independent SSL VPN gateways within a single appliance/cluster. This enables service providers to offer network-based SSL VPN managed services to multiple customers from a single device or cluster, as well as enabling enterprises to completely segment SSL VPN traffic between multiple groups. IVS enables complete customer separation and provides segregation of traffic between multiple customers using granular role based VLAN (802.1Q) tagging. This enables the secure segregation of end users’ traffic, even if two customers have overlapping IP addresses and enables provisioning of specific VLANs for different user constituencies, such as remote employees and partners of customers. DNS/WINS, AAA, log/accounting servers and application servers such as Web mail, file shares, etc. can reside either in the respective customers’ intranets or in the service provider network. Service providers 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, etc.

The IVS upgrade is available for the SA 4000 and SA 6000.

High Availability Option

Juniper Networks has designed a variety of HA clustering options to support the Secure Access appliances, ensuring redundancy and seamless failover in the rare case of a system failure. These clustering options also provide performance scalability to handle the most demanding usage scenarios. The Secure Access 2000 and 4000 can be purchased in Cluster Pairs and the Secure Access 6000 can be purchased in a Multi-Unit Clusters or Cluster Pairs, to provide complete redundancy and expansive user scalability. Both Multi-Unit Clusters and Cluster Pairs feature stateful peering and failover across the LAN and WAN, so in the unlikely event that one unit fails, system configurations (including authentication server, authorization groups, bookmarks, etc.), user profile settings (including user-defined bookmarks, cookies, etc.), and user sessions are preserved. Failover is seamless, so there is no interruption to user/enterprise productivity, no need for users to log in again, and no downtime. Multi-Unit Clusters are automatically deployed in Active/Active mode, while Cluster Pairs can be configured in either Active/Active or Active/Passive Mode.

The HA option is available for the SA 2000, SA 4000, and SA 6000.

ICE Option

SSL VPNs can help to keep organizations and businesses functioning by connecting people even during the most unpredictable circumstances – hurricanes, terrorist attacks, transportation strikes, pandemics or virus outbreaks, the result of which could mean the quarantine or isolation of entire regions or groups of people for an extended period of time. With the right balance of risk and cost, the new Juniper Networks Secure Access ICE offering delivers a timely solution for addressing a dramatic peak in demand for remote access to ensure business continuity whenever a disastrous event strikes. ICE provides licenses for a large number of additional users on a Secure Access SSL VPN appliance for a limited time. With ICE, businesses can:

- Maintain productivity by enabling ubiquitous access to applications and information for employees from anywhere, anytime, and any device

- Sustain partnerships with around the clock real-time access to applications and services while knowing resources are secured and protected
- Continue to deliver exceptional service to customers and partners with online collaboration
- Meet federal and government mandates for contingencies and continuity of operations (COOP) compliance
- Balance risk and scalability with cost and ease of deployment

The ICE license is available for the SA4000 and the SA6000 and includes all of the following features:

- Baseline
- Advanced
- Secure Application Manager and Network Connect
- Secure Meeting
- SSL Acceleration

Specifications

Dimensions and Power

	SA 2000	SA 4000	SA 6000
Dimensions (W x H x D)	16.7 x 1.7 x 15 in (42.4 x 4.4 x 38.1 cm)	16.7 x 1.7 x 15 in (42.4 x 4.4 x 38.1 cm)	16.7 x 3.5 x 16.2 in (42.4 x 8.9 x 41.2 cm)
Weight	13.2 lb (5.99 kg) typical (unboxed)	13.6 lb (6.17 kg) typical (unboxed)	28.5 lb (12.94 kg) typical (unboxed)
Rack Mountable	Yes, 19"	Yes, 19"	Yes, 19"
A/C Power Supply	100-240 VAC, 50-60 Hz, 2.5 A Max, 260 Watts	100-240 VAC, 50-60 Hz, 2.5 A Max, 260 Watts	100-240 VAC, 50-60 Hz, 2.5 A Max, 500 Watts
System Battery	CR2032 3 V lithium coin cell	CR2032 3 V lithium coin cell	CR2032 3 V lithium coin cell
Efficiency	65% minimum, at full load	65% minimum, at full load	65% minimum, at full load
MTBF	87,000 hours	70,000 hours	78,000 hours
Material	18 gauge (.048") cold-rolled steel	18 gauge (.048") cold-rolled steel	18 gauge (.048") cold-rolled steel
Fans	1 blower, 1-40 mm ball bearing fan in power supply	3-40 mm ball bearing fans, 1-40 mm ball bearing fan in power supply	2 externally accessible, hot swappable ball-bearing fans

Panel Display

Front Panel Power Button	Yes	Yes	Yes
Power LED, HD Activity, Temp	Yes	Yes	Yes
PS Fail	No	No	Yes
HDD Activity and RAID Status LEDs	No	No	Yes

Ports

Traffic	Two RJ-45 Ethernet – 10/100/1000 full or half-duplex (auto-negotiation)	Two RJ-45 Ethernet – 10/100/1000 full or half-duplex (auto-negotiation)	Two RJ-45 Ethernet – 10/100/1000 full or half-duplex (auto-negotiation) Two SFP ports – Gig-E
Management	N/A	N/A	One RJ-45 Ethernet-10/100/1000 full or half-duplex (auto-negotiation)
Fast Ethernet	IEEE 802.3u compliant	IEEE 802.3u compliant	IEEE 802.3u compliant
Gigabit Ethernet	IEEE 802.3z or IEEE 802.3ab compliant	IEEE 802.3z or IEEE 802.3ab compliant	IEEE 802.3z or IEEE 802.3ab compliant
Console	One 9-pin serial console port	One 9-pin serial console port	One 9-pin serial console port

Environment

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

Specifications

SA 2000

SA 4000

SA 6000

Certifications

Safety Certifications	EN60950-1:2001+ A11, UL60950-1:2003, CSA C22.2 No. 60950-1, IEC 60950-1:2001	EN60950-1:2001+ A11, UL60950-1:2003, CSA C22.2 No. 60950-1, IEC 60950-1:2001	EN60950-1:2001+ A11, UL60950-1:2003, CSA C22.2 No. 60950-1, IEC 60950-1:2001
Emissions Certifications	FCC Class A, VCCI Class A, CE class A	FCC Class A, VCCI Class A, CE class A	FCC Class A, VCCI Class A, CE class A
Common Criteria EAL2 Certification	Yes	Yes	Yes
FIPS Option (140-2, Level 3 Certification)	No	Yes	Yes
Warranty	90 days; Can be extended with support contract	90 days; Can be extended with support contract	90 days; Can be extended with support contract

Ordering Information

Secure Access 2000 Base System

SA2000	Secure Access 2000 Base System
--------	--------------------------------

Secure Access 2000 User Licenses

SA2000-ADD-25U	Add 25 simultaneous users to SA 2000
SA2000-ADD-50U	Add 50 simultaneous users to SA 2000
SA2000-ADD-100U	Add 100 simultaneous users to SA 2000

Secure Access 2000 Feature Licenses

SA2000-SAMNC	Secure Application Manager and Network Connect for SA 2000
SA2000-ADV	Advanced for SA 2000
SA2000-MTG	Secure Meeting for SA 2000
SA-AED-ADD-50U	Advanced Endpoint Defense: Malware Protection - Add 50 simultaneous users
SA-AED-ADD-100U	Advanced Endpoint Defense: Malware Protection - Add 100 simultaneous users

Secure Access 2000 Clustering Licenses

SA2000-CL-25U	Clustering: Allow 25 additional users to be shared from another SA 2000
SA2000-CL-50U	Clustering: Allow 50 additional users to be shared from another SA 2000
SA2000-CL-100U	Clustering: Allow 100 additional users to be shared from another SA 2000

Secure Access 4000 Base System

SA4000	Secure Access 4000 Base System
--------	--------------------------------

Secure Access 4000 User Licenses

SA4000-ADD-50U	Add 50 simultaneous users to SA 4000
SA4000-ADD-100U	Add 100 simultaneous users to SA 4000
SA4000-ADD-250U	Add 250 simultaneous users to SA 4000
SA4000-ADD-500U	Add 500 simultaneous users to SA 4000
SA4000-ADD-1000U	Add 1000 simultaneous users to SA 4000

Secure Access 4000 Feature Licenses

SA4000-SAMNC	Secure Application Manager and Network Connect for SA 4000
SA4000-ADV	Advanced for SA 4000
SA4000-MTG	Secure Meeting for SA 4000
SA4000-SSL	SSL Acceleration License for SA 4000
SA4000-IVS	Instant Virtual System for SA 4000
SA-AED-ADD-50U	Advanced Endpoint Defense: Malware Protection - Add 50 simultaneous users
SA-AED-ADD-100U	Advanced Endpoint Defense: Malware Protection - Add 100 simultaneous users
SA-AED-ADD-250U	Advanced Endpoint Defense: Malware Protection - Add 250 simultaneous users
SA-AED-ADD-500U	Advanced Endpoint Defense: Malware Protection - Add 500 simultaneous users

Secure Access 4000 Clustering Licenses

SA4000-CL-50U	Clustering: Allow 50 additional users to be shared from another SA 4000
SA4000-CL-100U	Clustering: Allow 100 additional users to be shared from another SA 4000
SA4000-CL-250U	Clustering: Allow 250 additional users to be shared from another SA 4000
SA4000-CL-500U	Clustering: Allow 500 additional users to be shared from another SA 4000
SA4000-CL-1000U	Clustering: Allow 1000 additional users to be shared from another SA 4000

Secure Access 6000 Base System

SA6000	Secure Access 6000 Base System
--------	--------------------------------

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 SA 6000s required

Secure Access 6000 Feature Licenses

SA6000-SAMNC	Secure Application Manager and Network Connect for SA 6000
SA6000-ADV	Advanced for SA 6000
SA6000-MTG	Secure Meeting for SA 6000
SA6000-IVS	Instant Virtual System for SA 6000
SA-AED-ADD-50U	Advanced Endpoint Defense: Malware Protection - Add 50 simultaneous users
SA-AED-ADD-100U	Advanced Endpoint Defense: Malware Protection - Add 100 simultaneous users
SA-AED-ADD-250U	Advanced Endpoint Defense: Malware Protection - Add 250 simultaneous users
SA-AED-ADD-500U	Advanced Endpoint Defense: Malware Protection - Add 500 simultaneous users
SA-AED-ADD-1000U	Advanced Endpoint Defense: Malware Protection - Add 1000 simultaneous users
SA-AED-ADD-2500U	Advanced Endpoint Defense: Malware Protection - Add 2500 simultaneous users

Ordering Information cont'd

Secure Access 6000 Clustering Licenses

SA6000-CL-100U	Clustering: Allow 100 additional users to be shared from another SA 6000
SA6000-CL-250U	Clustering: Allow 250 additional users to be shared from another SA 6000
SA6000-CL-500U	Clustering: Allow 500 additional users to be shared from another SA 6000
SA6000-CL-1000U	Clustering: Allow 1000 additional users to be shared from another SA 6000
SA6000-CL-2500U	Clustering: Allow 2500 additional users to be shared from another SA 6000
SA6000-CL-5000U	Clustering: Allow 5000 additional users to be shared from another SA 6000
SA6000-CL-7500U	Clustering: Allow 7500 additional users to be shared from another SA 6000
SA6000-CL-10000U	Clustering: Allow 10000 additional users to be shared from another SA 6000
SA6000-CL-12500U	Clustering: Allow 12500 additional users to be shared from another SA 6000
SA6000-CL-15000U	Clustering: Allow 15000 additional 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-1U	Spare Secure Access Rack Mount Kit-1U
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 SA 6000
SA6000-GBIC-FLX	GBIC Transceiver-Fiber LX for SA 6000
SA6000-GBIC-COP	GBIC Transceiver-Copper for SA 6000

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.



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

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.

100189-004 Nov 2007

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