Juniper Networks Secure Access 2500, 4500 and 6500 Appliances

Juniper Networks Secure Access SSL VPN products lead the SSL virtual private network (VPN) market with a complete range of remote access appliances, including the new, next-generation Secure Access 2500 (SA 2500), Secure Access 4500 (SA 4500), and Secure Access 6500 (SA 6500) with its high scalability and redundancy capabilities that are specifically designed for large enterprises and service providers. 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 SSL VPN appliances deliver lower total cost of ownership over traditional IPSec client solutions and unique end-to-end security features.

Product Description

Juniper Networks introduces the next generation of its market-leading Secure Access SSL VPN appliances. The new SA 2500, SA 4500 and SA 6500 are SSL VPN appliances that meet the needs of companies of all sizes. With the SA 6500, Juniper continues to demonstrate its SSL VPN market leadership by delivering a highly scalable solution based on real-world performance testing. Secure Access appliances use SSL, the security protocol found in all standard Web browsers. The use of SSL eliminates the need for pre-installed client software, changes to internal servers, and costly ongoing maintenance and desktop support. Juniper's Secure Access SSL VPN appliances also offer sophisticated partner/customer extranet features that enable controlled access to differentiated users and groups without requiring infrastructure changes, demilitarized zone (DMZ) deployments or software agents.

Architecture and Key Components

The Juniper Networks SA 2500 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 2500 offers High Availability (HA) with seamless user failover. And because the SA 2500 runs the exact same software as the larger SA 4500 and SA 6500, even smaller organizations gain the same high-performance, administrative flexibility and end user experience.

The Juniper Networks SA 4500 enables mid-to-large size organizations to provide cost effective extranet access to remote employees and partners using only a Web browser. The SA 4500 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 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 4500 also offers HA with seamless user failover.

The Juniper Networks SA 6500 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 6500 offers HA with seamless user failover. The SA 6500 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.

Because each of the Juniper Networks Secure Access SSL VPN devices runs on the same software, there is no need to compromise user or administrator experience based on which one you choose. All devices offer leading performance, stability and scalability. Therefore, deciding which device will best fit the needs of your organization is easily determined by matching the required number of concurrent users, and perhaps system redundancy and large-scale acceleration options, to the needs of your growing remote access user population.

- **SA 2500:** Supports small-to-medium-size business (SMBs) as a cost-effective solution that can easily handle up to 100 concurrent users on a single system or 2-unit cluster.

- **SA 4500:** Enables mid-to-large size organizations to grow to as many as 1,000 concurrent users on a single system and offers the option to upgrade to hardware-based SSL acceleration for those that demand the most performance available under heavy load.

- **SA 6500:** Purpose-built for large enterprises and service providers, the SA 6500 features best-in-class performance, scalability and redundancy for organizations with high volume secure access and authorization requirements, with support for as many as 10,000 concurrent users on a single system or tens of thousands of concurrent users across a 4-unit cluster.

SA 6500 Standard Features
- Dual, mirrored hot swappable Serial Advanced Technology Attachment (SATA) hard drives
- Dual, hot swappable fans
- Dual, redundant hot swappable power supplies
- 4 GB SDRAM
- 4-port copper 10/100/1000 interface card
- 1-port copper 10/100/1000 management interface
- Hardware-based SSL acceleration module

SA 6500 Optional Features
- DC power supply available
- 4-port Small Form-factor Pluggable (SFP) interface card

Features and Benefits

High Scalability Support on Secure Access 6500 SSL VPN
The SA 6500 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 shows the number of concurrent users that can be supported on the SA 6500 platform:

- Single SA 6500: Supports up to 10,000 concurrent users
- Two-unit cluster of SA 6500s: Supports up to 18,000 concurrent users
- Three-unit cluster of SA 6500s: Supports up to 26,000 concurrent users
- Four-unit cluster of SA 6500s: Supports up to 30,000 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 2500, SA 4500 and SA 6500 provide complete end-to-end layered security, including endpoint client, device, data and server layered security controls.

Table 1: End-to-End Layered Security Features and Benefits

Feature	Feature Description	Benefits
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, and so on). 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.	Uses 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 in 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.

Feature	Feature Description	Benefits
Hardened Security Appliance	Designed on a purpose-built operating system.	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	A secure and separate environment for remote sessions that encrypts all data and controls I/O access (printers, drives).	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 like cookies, headers and form entries) from leaving the network.
Integrated Malware Protection	Pre-installed checks to protect users and devices from keyloggers, Trojans and remote control applications.	Enables customers to provision endpoint containment capabilities.
Coordinated Threat Control	Enables Juniper's Secure Access 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 identifies, stops and remediates both network and application-level threats within remote access traffic.

Lower Total Cost of Ownership

In addition to enterprise-class security benefits, the SA 2500, SA 4500 and SA 6500 have a wealth of features that enable low total cost of ownership.

Table 2: Cost of Ownership Features and Benefits

Feature	Feature Description	Benefits
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, no 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 is 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, Security Assertion Markup Language (SAML), and public key infrastructure (PKI)/ digital certificates.	Leverages existing corporate authentication methods to simplify administration.
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.
Juniper Networks Central Manager	Intuitive Web-based user interface (UI) for configuring, updating and monitoring SA appliances within a single device/cluster or across a global cluster deployment.	Enables companies to conveniently manage, configure and maintain SA appliances from one central location.
"In Case of Emergency" (ICE)	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.
Cross-platform Support	Ability for any platform to gain access to resources such as Windows, Mac, Linux or 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 2500, SA 4500 and SA 6500 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 users log into 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 restrictions.

Table 3: Access Privilege Management Features and Benefits

Feature	Feature Description	Benefits
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 can be 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	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.
Custom Expressions	Enables the dynamic combination of attributes on a "per-session" basis, at the role definition/mapping rules and the resource authorization policy level.	Enables finer granularity and customization of policy roles.

User Self-Service

The SA 2500, SA 4500 and SA 6500 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.

Table 4: User Self-Service Features and Benefits

Feature	Feature Description	Benefits
Password Management Integration	Standards-based interface for extensive integration with password policies in directory stores (LDAP, Microsoft Active Directory, NT, and others)	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 NT LAN Manager (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	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 2500, SA 4500 and SA 6500 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.

Table 5: Provisioning Features and Benefits

Feature	Feature Description	Benefits
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.

Product Options

The SA 2500, SA 4500 and SA 6500 hardware include various license options for greater functionality.

User License

With the release of the SA 2500, 4500 and 6500 appliances, purchasing has been simplified, thanks to a combination of features that were once separate upgrades. Now there is only one license that is needed to get started: the User licenses. Current customers with the older generation hardware (SA 2000, 4000 and 6000) will also benefit from these changes as systems are upgraded to version 6.1 (or higher) software.

User licenses provide the functionality that allows the remote, extranet and intranet user to access the network. They fully meet the needs of both basic and complex deployments with diverse audiences and use cases, and require little or no client software, server changes, DMZ build-outs or software agent deployments. And for administrative ease of user license counts, each license only enables as many users as specified in the license and are additive. For example, if a 100 user license was originally purchased and the concurrent user count grows over the next year to exceed that amount, simply adding another 100 user license to the system will now allow for up to 200 concurrent users. Key features enabled by this license include:

- Secure Application Manager (SAM) and Network Connect (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 provides secure access to virtually any audience, from remote/mobile workers to partners or customers, using a wide range of devices from any network.

- Provision by purpose goes beyond role-based access controls and allows administrators to properly, accurately and dynamically balance security concerns with access requirements.

- Advanced PKI support includes the ability to import multiple root and intermediate CAs, Online Certificate Status Protocol (OCSP), and multiple server certificates.

- User self-service provides the ability for users to create their own favorite bookmarks, including accessing their own workstation from a remote location, and even changing their password when it is set to expire.

- Multiple hostname support (for example, https://employees.company.com, https://partners.company.com and https://employees.company.com/engineering) can all be made to look as though they are the only ones using the system, complete with separate logon pages and customized views that uniquely target the needs and desires of that audience.

- Customizable UI for users and delegated administrative roles.

- Advanced endpoint security controls such as Host Checker, Cache Cleaner and Secure Virtual Workspace work to ensure that users are dynamically provisioned to access systems and resources only to the degree that their remote systems are compliant with the organization's security policy, after which remnant data is scrubbed from the hard drive so that nothing is left behind.

- VLAN support of up to 240 VLANs.

Advanced Endpoint Defense: Integrated Malware Protection License (Optional)

Advanced Endpoint Defense: Malware Protection is an endpoint security software module that integrates with Host Checker and provides protection from unwanted malware such as Trojans and keyloggers 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 preinstall. All Secure Access SSL VPN 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 2500, SA 4500 and SA 6500.

Secure Meeting License (Optional)

The Secure Meeting upgrade license extends the capabilities of the Juniper Networks Secure Access SSL VPN appliances by providing secure any time, anywhere, cost-effective online Web conferencing and remote control PC access. Secure Meeting enables real-time application sharing so that 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 2500, SA 4500 and SA 6500.

Instant Virtual System License (Optional)

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 user 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. Domain Name Service (DNS)/Windows Internet Name Service (WINS), AAA, log/accounting servers and application servers such as Web mail and file shares to name a few, can reside either in the respective customer's 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 to different user audiences such as remote employees, contractors, partners and others.

The IVS upgrade is available for the SA 4500 and SA 6500.

High Availability License (Optional)

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 2500 and 4500 can be purchased in Cluster Pairs and the Secure Access 6500 can be purchased in 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 (like authentication server, authorization groups and bookmarks), user profile settings (like user-defined bookmarks and cookies), 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.

High Availability licenses allow you to share licenses from one Secure Access appliance with one or more additional Secure Access appliances (depending on the platform in question) and are not additive to the concurrent user licenses. For example, if a customer has a 100 user license for the SA 4500 and then purchases another SA 4500 with a 100 user cluster license, this will provide a total of 100 users that are shared across both appliances, not per appliance.

The HA option is available for the SA 2500, SA 4500 and SA 6500.

ICE License (Optional)

SSL VPNs can help 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, at any time, and on 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 SA 4500 and the SA 6500 and includes the following features:

- Baseline
- Secure Meeting

Specifications

	SA 2500	SA 4500	SA 6500
Dimensions and Power			
Dimensions (W x H x D)	17.26 x 1.75 x 14.5 in (43.8 x 4.4 x 36.8 cm)	17.26 x 1.75 x 14.5 in (43.8 x 4.4 x 36.8 cm)	17.26 x 3.5 x 17.72 in (43.8 x 8.8 x 45 cm)
Weight	14.6 lb (6.6 kg) typical (unboxed)	15.6 lb (7.1 kg) typical (unboxed)	26.4 lb (12 kg) typical (unboxed)
Rack Mountable	Yes, 1U	Yes, 1U	Yes, 2U, 19 inch
A/C Power Supply	100-240 VAC, 50-60 Hz, 2.5 A Max, 200 Watts	100-240 VAC, 50-60 Hz, 2.5 A Max, 300 Watts	100-240 VAC, 50-60 Hz, 2.5 A Max, 400 Watts
System Battery	CR2032 3V lithium coin cell	CR2032 3V lithium coin cell	CR2032 3V lithium coin cell
Efficiency	80% minimum, at full load	80% minimum, at full load	80% minimum, at full load
Material	18 gauge (.048") cold-rolled steel	18 gauge (.048") cold-rolled steel	18 gauge (.048 in) cold-rolled steel
Fans	Three 40mm ball bearing fans, One 40mm ball bearing fan in power supply	Three 40mm ball bearing fans, One 40mm ball bearing fan in power supply	Two 80mm hot swap, One 40mm ball bearing fan in power supply
Panel Display			
Power LED, HD Activity, HW Alert	Yes	Yes	Yes
HD Activity and Fail LED on Drive Tray	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)	Four RJ-45 Ethernet – full or half-duplex (auto-negotiation) SFP module optional
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 RJ-45 serial console port	One RJ-45 serial console port	One 9-pin serial console port
Environment			
Operating Temp	41° to 104° F (5° to 40° C)	41° to 104° F (5° to 40° C)	41° to 104° F (5° to 40° C)
Storage Temp	-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)	10,000 ft (3,000 m) maximum	10,000 ft (3,000 m) maximum	10,000 ft (3,000 m) maximum
Altitude (storage)	40,000 ft (10,600 m) maximum	40,000 ft (10,600 m) maximum	40,000 ft (10,600 m) maximum
Certifications			
Safety Certifications	EN60950-1:2001+ A11, UL60950-1:2003, CAN/CSA C22.2 No. 60950-1-03, IEC 60950-1:2001	EN60950-1:2001+ A11, UL60950-1:2003, CAN/CSA C22.2 No. 60950-1-03, IEC 60950-1:2001	EN60950-1:2001+ A11, UL60950-1:2003, CAN/CSA C22.2 No. 60950-1-03, IEC 60950-1:2001
Emissions Certifications	FCC Class A, EN 55022 Class A, EN 55024 Immunity, EN 61000-3-2, VCCI Class A	FCC Class A, EN 55022 Class A, EN 55024 Immunity, EN 61000-3-2, VCCI Class A	FCC Class A, EN 55022 Class A, EN 55024 Immunity, EN 61000-3-2, VCCI Class A
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

Model Number	Description
Secure Access 2500 Base System	
SA2500	Secure Access 2500 Base System
Secure Access 2500 User Licenses	
SA2500-ADD-10U	Add 10 simultaneous users to SA 2500
SA2500-ADD-25U	Add 25 simultaneous users to SA 2500
SA2500-ADD-50U	Add 50 simultaneous users to SA 2500
SA2500-ADD-100U	Add 100 simultaneous users to SA 2500
Secure Access 2500 Feature Licenses	
SA2500-MTG	Secure Meeting for SA 2500
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 2500 Clustering Licenses	
SA2500-CL-10U	Clustering: Allow 10 additional users to be shared from another SA 2500
SA2500-CL-25U	Clustering: Allow 25 additional users to be shared from another SA 2500
SA2500-CL-50U	Clustering: Allow 50 additional users to be shared from another SA 2500
SA2500-CL-100U	Clustering: Allow 100 additional users to be shared from another SA 2500
Secure Access 4500 Base System	
SA4500	Secure Access 4500 Base System
Secure Access 4500 User Licenses	
SA4500-ADD-50U	Add 50 simultaneous users to SA 4500
SA4500-ADD-100U	Add 100 simultaneous users to SA 4500
SA4500-ADD-250U	Add 250 simultaneous users to SA 4500
SA4500-ADD-500U	Add 500 simultaneous users to SA 4500
SA4500-ADD-1000U	Add 1000 simultaneous users to SA 4500
Secure Access 4500 Feature Licenses	
SA4500-MTG	Secure Meeting for SA 4500
SA4500-IVS	Instant Virtual System for SA 4500
SA4500-ICE	In Case of Emergency License for SA 4500
SA4500-ICE-CL	In Case of Emergency Clustering License for SA 4500
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

Model Number	Description
Secure Access 4500 Clustering Licenses	
SA4500-CL-50U	Clustering: Allow 100 additional users to be shared from another SA 4500
SA4500-CL-100U	Clustering: Allow 25 additional users to be shared from another SA 2500
SA4500-CL-250U	Clustering: Allow 250 additional users to be shared from another SA 4500
SA4500-CL-500U	Clustering: Allow 500 additional users to be shared from another SA 4500
SA4500-CL-1000U	Clustering: Allow 1000 additional users to be shared from another SA 4500
Secure Access 6500 Base System	
SA6500	Secure Access 6500 Base System
Secure Access 6500 User Licenses	
SA6500-ADD-100U	Add 100 simultaneous users to SA 6500
SA6500-ADD-250U	Add 250 simultaneous users to SA 6500
SA6500-ADD-500U	Add 500 simultaneous users to SA 6500
SA6500-ADD-1000U	Add 1000 simultaneous users to SA 6500
SA6500-ADD-2500U	Add 2500 simultaneous users to SA 6500
SA6500-ADD-5000U	Add 5000 simultaneous users to SA 6500
SA6500-ADD-7500U	Add 7500 simultaneous users to SA 6500
SA6500-ADD-10000U	Add 10000 simultaneous users to SA 6500
SA6500-ADD-12500U*	Add 12500 simultaneous users to SA 6500
SA6500-ADD-15000U*	Add 15000 simultaneous users to SA 6500
SA6500-ADD-20000U*	Add 20000 simultaneous users to SA 6500
SA6500-ADD-25000U*	Add 25000 simultaneous users to SA 6500
SA6500-ADD-25000U*	Add 25000 simultaneous users to SA 6500
*Multiple SA 6500s required	
Secure Access 6500 Feature Licenses	
SA6500-MTG	Secure Meeting for SA 6500
SA6500-IVS	Instant Virtual System for SA 6500
SA6500-ICE	In Case of Emergency License for SA 6500
SA6500-ICE-CL	In Case of Emergency Clustering License for SA 6500
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

Model Number	Description
Secure Access 6500 Clustering Licenses	
SA6500-CL-100U	Clustering: Allow 100 additional users to be shared from another SA 6500
SA6500-CL-250U	Clustering: Allow 250 additional users to be shared from another SA 6500
SA6500-CL-500U	Clustering: Allow 500 additional users to be shared from another SA 6500
SA6500-CL-1000U	Clustering: Allow 1000 additional users to be shared from another SA 6500
SA6500-CL-2500U	Clustering: Allow 2500 additional users to be shared from another SA 6500
SA6500-CL-5000U	Clustering: Allow 5000 additional users to be shared from another SA 6500
SA6500-CL-7500U	Clustering: Allow 7500 additional users to be shared from another SA 6500
SA6500-CL-10000U	Clustering: Allow 10000 additional users to be shared from another SA 6500
SA6500-CL12500U	Clustering: Allow 12500 additional users to be shared from another SA 6500
SA6500-CL-15000U	Clustering: Allow 15000 additional users to be shared from another SA 6500
SA6500-CL-20000U	Clustering: Allow 20000 additional users to be shared from another SA 6500
SA6500-CL-25000U	Clustering: Allow 25000 additional users to be shared from another SA 6500
Accessories	
SA4500-CRYPTO	Field Upgradeable SSL Acceleration Module for SA 4500
SA6500-PS	Field Upgradeable Secondary Power Supply for SA 6500
SA6500-HD	Field Replaceable Hard Disk for SA 6500
SA6500-FAN	Field Replaceable Fan for SA 6500
SA2500-4500-ACC-RKMT-1U	Secure Access and Infranet Controller Rack Mount Kit - 1U
SA6500-ACC-RKMT-2U	Secure Access and Infranet Controller Rack Mount Kit - 2U
SA6500-GBIC-FSX	GBIC Transceiver-Fiber SX for SA 6500
SA6500-GBIC-FLX	GBIC Transceiver-Fiber LX for SA 6500
SA6500-GBIC-COP	GBIC Transceiver-Copper for SA 6500
SA6500-IOC	GBIC I/O Card

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

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