



# SA SERIES SSL VPN APPLIANCES

SA2500, SA4500, SA6500

## Product Overview

The Juniper Networks SA2500, SA4500, and SA6500 SSL VPN Appliances meet the needs of companies of all sizes. With the SA6500, Juniper continues to demonstrate its SSL VPN market leadership by delivering a highly scalable solution based on real-world performance. Juniper Networks SA Series SSL VPN Appliances lead the SSL VPN market with a complete range of remote access appliances. The SA Series now includes Junos Pulse which provides a simple, intuitive client that provides secure, authenticated access for remote users from any Web-enabled device to corporate resources. The SA Series combines 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 SA Series SSL VPN Appliances deliver lower total cost of ownership over traditional IPsec client solutions and unique end-to-end security features.

## Product Description

The Juniper Networks® SA2500, SA4500, and SA6500 SSL VPN Appliances meet the needs of companies of all sizes. With the SA6500, Juniper continues to demonstrate its SSL VPN market leadership by delivering a highly scalable solution based on real-world performance testing. SA Series SSL VPN 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 Networks SA Series also offers 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.

The SA Series now includes Juniper Networks Junos® Pulse, a dynamic, integrated, multi-service network client for mobile and non-mobile devices. Junos Pulse enables optimized, accelerated anytime, anywhere access to corporate data. Pulse enables secure SSL access from a wide range of mobile and non-mobile devices, including smartphones, netbooks, notebooks, Wi-Fi or 3G-enabled devices. Junos Pulse delivers enterprises improved productivity and secure, ubiquitous access to corporate data and applications, anytime, anywhere. For more details on Junos Pulse, please visit [www.juniper.net/us/en/products-services/software/junos-platform/junos-pulse/](http://www.juniper.net/us/en/products-services/software/junos-platform/junos-pulse/).

## Architecture and Key Components

The SA2500 SSL VPN Appliance 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 SA2500 offers high availability (HA) with seamless user failover. And because the SA2500 runs the exact same software as the larger SA4500 and SA6500, even smaller organizations gain the same high-performance, administrative flexibility, and end user experience.

The SA4500 SSL VPN Appliance enables mid-to-large size organizations to provide cost-effective extranet access to remote employees and partners using only a Web browser. SA4500 features 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 use 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 SA4500 also offers HA with seamless user failover.

The SA6500 SSL VPN Appliance 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 SA6500 offers HA with seamless user failover. The SA6500 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 SA Series SSL VPN Appliances 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.

- **SA2500:** Supports SMBs as a cost-effective solution that can easily handle up to 100 concurrent users on a single system or two-unit cluster.
- **SA4500:** 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.

- **SA6500:** Purpose-built for large enterprises and service providers, the SA6500 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 four-unit cluster.

#### SA6500 Standard Features

- Dual, mirrored hot swappable Serial Advanced Technology Attachment (SATA) hard drives
- Dual, hot swappable fans
- Hot swappable power supply
- 4 gigabyte SDRAM
- 4-port copper 10/100/1000 interface card
- 1-port copper 10/100/1000 management interface
- Hardware-based SSL acceleration module

#### SA6500 Optional Features

- Second power supply or DC power supply available
- 4-port small form-factor pluggable (SFP) interface card

#### Features and Benefits

##### Junos Pulse

Junos Pulse is an integrated, multi-service network client enabling anytime, anywhere connectivity, security, and acceleration with a simplified user experience that requires minimal user interaction. Junos Pulse makes secure network and cloud access easy through virtually any device – mobile or non-mobile, Wi-Fi or 3G-enabled, managed or unmanaged – over a broad array of computing and mobile operating systems. The following table provides the key features and benefits of Junos Pulse working with the SA Series appliances.

FEATURES	BENEFITS
Layer 3 SSL VPN (Network Connect)	<ul style="list-style-type: none"> <li>• Layer 3 VPN connectivity with granular access control</li> <li>• SSL mode only; no ESP (Encapsulating Security Payload) mode</li> </ul>
Location awareness	<ul style="list-style-type: none"> <li>• Seamless roaming from remote access (to Juniper SA Series) to local LAN access (via Juniper UAC)</li> <li>• Junos Pulse can be pre-configured by admins to automatically prompt end-users for credentials to authenticate to the SA Series when they are remote</li> </ul>
Endpoint security	<ul style="list-style-type: none"> <li>• Full Host Checker capability to check endpoint security</li> <li>• Enhanced Endpoint Security delivers on-the-fly malware protection, pre-connection scanning policies, and real-time protection supported by both the SA Series and UAC</li> </ul>
Split tunneling options (enable or disable without route monitoring)	<ul style="list-style-type: none"> <li>• Key split tunneling options of Network Connect supported</li> <li>• Enforces secure, granular access control</li> </ul>
Flexible launch options (standalone client, browser-based launch)	<ul style="list-style-type: none"> <li>• Users can easily launch Junos Pulse via the web from the SA Series landing page</li> <li>• Remote users can simply launch Junos Pulse from their desktop</li> </ul>
Pre-configuration options (pre-configured installer to contain list of SA Series appliances)	<ul style="list-style-type: none"> <li>• Admins can pre-configure a Junos Pulse deployment with a list of corporate SA Series appliances for end-users to choose from</li> </ul>
Connectivity options (max/idle session timeouts, automatic reconnect, logging)	<ul style="list-style-type: none"> <li>• Admins can set up flexible connectivity options for remote users</li> </ul>

For more details on Junos Pulse, please visit [www.juniper.net/us/en/products-services/software/junos-platform/junos-pulse/](http://www.juniper.net/us/en/products-services/software/junos-platform/junos-pulse/).

## High Scalability Support on SA6500 SSL VPN Appliance

The SA6500 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 list shows the number of concurrent users that can be supported on the SA6500 platform:

- Single SA6500: Supports up to 10,000 concurrent users
- Two-unit cluster of SA6500s: Supports up to 18,000 concurrent users

- Three-unit cluster of SA6500s: Supports up to 26,000 concurrent users
- Four-unit cluster of SA6500s: 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.

## End-to-End Layered Security

The SA2500, SA4500, and SA6500 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
Antimalware support with Enhanced Endpoint Security	Dynamically download Webroot's market-leading antimalware software to enforce endpoint security on devices which may not be corporate-assigned computers being used for network access.	Protects endpoints from infection in real-time from antimalware and thereby protects corporate resources from harm during network access. Enables dynamic enforcement of antimalware protection on unmanaged assets, such as PC's of external partners, customers or suppliers.
SMS auto-remediation	Automatically remediates non-compliant endpoints by updating software applications that do not comply to corporate security policies. Dynamically initiates an update of these software applications on the endpoint using Microsoft's SMS protocol.	Improves productivity of remote users who will gain immediate access to the corporate network without having to wait for periodic updates of software applications, and ensures compliance with corporate security policies.
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, other). 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. Includes cache cleaner that erases all proxy downloads and temp files at logout.	Verifies/ensures that endpoint device meets corporate security policy requirements before granting access, remediating devices, and quarantining users when necessary. Also, ensures no potentially sensitive data is left behind on the endpoint device.
Host Checker 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.
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 with 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 unsecure kiosks after a session.
Coordinated threat control	Enables SA Series SSL VPN Appliances and Juniper Networks IDP Series Intrusion Detection and Prevention Appliances to tie the session identity of the SSL VPN with the threat detection capabilities of the IDP Series, taking automatic action on users launching attacks.	Effectively identifies, stops, and remediates both network and application-level threats within remote access traffic.

## Ease of Administration

In addition to enterprise-class security benefits, the SA2500, SA4500, and SA6500 have a wealth of features that make it easy for the administrator to deploy and manage.

Table 2: Ease of Administration Features and Benefits

FEATURE	FEATURE DESCRIPTION	BENEFITS
Bridge CA (Certificate Authority) support	Enables the SA Series to support federated PKI deployments with client certificate authentication. Bridge CA is a PKI extension (as specified in RFC 5280) to cross-certify client certificates that are issued by different trust anchors (Root CAs). Also, enables the customer to configure policy extensions in the SA Series admin UI, to enforce during certificate validation. These policy extensions can be configured as per RFC 5280 guidelines.	Enables customers who use advanced PKI deployments to deploy the SA Series to perform strict standards-compliant certificate validation, before allowing data and applications to be shared between organizations and users.
Based on industry standard protocols and security methods	No installation or deployment of proprietary protocols is required.	SA Series investment 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 APIs for directory integration, as they are 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 websites from a single SA Series SSL VPN 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 Network and Security Manager (NSM)	Intuitive centralized UI for configuring, updating, and monitoring SA Series appliances within a single device/cluster or across a global cluster deployment.	Enables companies to conveniently manage, configure and maintain SA Series appliances and other Juniper devices from one central location.
In Case of Emergency (ICE)	Provides licenses for a large number of additional users on an SA Series 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 such as Windows, Mac, Linux or various mobile devices including iPhone, WinMobile, Symbian, and Android.	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 SA2500, SA4500, and SA6500 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 Series SSL VPN 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
UAC-SA federation	Seamlessly provision SA Series user sessions into Juniper Networks Unified Access Control upon login – or the alternative (provisioning of UAC sessions into the SA Series). Users need to authenticate only one time to get access in these types of environments.	Provides users – whether remote or local – seamless access with a single login to corporate resources that are protected by access control policies from UAC or the SA Series. Simplifies end user experience.
Certificate authentication to backend servers	Enables customers to enforce client authentication on their secure backend servers and allows the SA to present an admin-configured certificate to these servers for authentication.	Allows customers to mandate strict SSL policies on their backend servers by configuring client authentication.

FEATURE	FEATURE DESCRIPTION	BENEFITS
Client cert auth for ActiveSync	Any mobile device supporting ActiveSync along with client side certificates can now be challenged by the SA Series for a valid client certificate before being allowed access to the ActiveSync server.	Enables the administrator to enforce strict mobile authentication policies for ActiveSync access from mobile devices.
Multiple sessions per user	Allows remote users to launch multiple sessions to the SA Series appliance.	Enables remote users to have multiple authenticated sessions open at the same time.
User-record synchronization	Supports synchronization of user records such as user bookmarks across different non-clustered SA Series appliances.	Ensures ease of experience for users who often travel from one region to another and therefore need to connect to different SA Series appliances.
VDI (Virtual Desktop Infrastructure) support	Allows interoperability with VMware View Manager and Citrix XenDesktop to enable administrators to deploy virtual desktops with the SA Series appliances.	Provides seamless access to remote users to their virtual desktops hosted on VMware or Citrix servers. Provides dynamic delivery of the Citrix ICA client or the VMware View client, including dynamic client fallback options to allow users to easily connect to their virtual desktops.
ActiveSync feature	Provides secure access connectivity from mobile devices (such as Symbian, Windows Mobile, or iPhone) to the Exchange server with no client software installation. Enables up to 5000 simultaneous sessions on the SA6500.	Enables customers to allow a large number of users including employees, contractors and partners to access corporate resources through mobile phones via ActiveSync.
Dynamic role mapping with custom expressions	Combines network, device, and session attributes to determine which types of access are allowed. A dynamic combination of attributes on a per-session basis can be used to make the role mapping decision.	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, for different roles of users.	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.

## Flexible Single Sign-On (SSO) Capabilities

The SA2500, SA4500, and SA6500 offer comprehensive single sign-on 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: Flexible Single Sign-on Features and Benefits

FEATURE	FEATURE DESCRIPTION	BENEFITS
Kerberos Constrained Delegation	Support for Kerberos Constrained Delegation protocol. When a user logs into the SA Series with a credential that cannot be proxied through to the backend server, the SA Series appliance will retrieve a Kerberos ticket on behalf of the user from the Active Directory infrastructure. The ticket will be cached on the SA Series appliance throughout the session. When the user accesses Kerberos-protected applications, the SA Series will use the cached Kerberos credentials to log the user into the application without prompting for a password.	Eliminates the need for companies to manage static passwords resulting in reduced administration time and costs.
Kerberos SSO and NTLMv2 support	SA Series will automatically authenticate remote users via Kerberos or NTLMv2 using user credentials.	Simplifies user experience by avoiding having users enter credentials multiple times to access different applications.
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 Series 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 SA2500, SA4500, and SA6500 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
IPsec/IKEv2 support for mobile devices	Allows remote users to connect from devices such as PDA's, mobile devices and smartphones which support IKEv2 VPN connectivity. Administrator can also enable strict certificate authentication for access via IPsec/IKEv2.	Extends Juniper's leading mobility and access control features of SA Series to broad range of devices and OS platforms that support IKEv2 VPN connectivity. Enables remote users to securely authenticate to the SA Series appliance from platforms that support IKEv2 VPN connectivity.
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. Allows for split tunneling capability.	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 Networks Installer Services, no admin rights are needed to install, run, and upgrade Network Connect; optional standalone installation is available as well. Split tunneling capability provides flexibility to specify which subnets or hosts to include or exclude from being tunneled.
Junos Pulse	Single, integrated remote access client that can also provide LAN access control, WAN acceleration and Dynamic VPN features to remote users, in conjunction with Juniper Networks UAC, WXC Series Application Acceleration Platforms and SRX Series Services Gateways devices respectively.	Pulse replaces the need to deploy and maintain multiple, separate clients for different functionalities – such as VPN, LAN access control and WAN acceleration. By seamlessly integrating all these functionalities into one single, easy-to-use client, administrators can save on client management and deployment costs to end users.

## Product Options

The SA2500, SA4500, and SA6500 appliances include various license options for greater functionality.

### User License

With the release of the SA2500, SA4500, and SA6500 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 (Juniper Networks SA2000, SA4000, and SA6000) 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:

- Junos Pulse, SAM and Network Connect provide cross-platform support for client/server applications using SAM, as well as full network-layer access using the SSL transport mode of Junos Pulse and the adaptive dual transport methods of Network Connect. The combination of SAM, Junos Pulse and Network Connect 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 certificate authorities (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 users 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.
- User interfaces are customizable 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.
- Provides support of up to 240 VLANs.

### Secure Meeting License (Optional)

The Juniper Networks Secure Meeting upgrade license extends the capabilities of the SA Series SSL VPN Appliances by providing secure anytime, 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 his/her 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 SA2500, SA4500, and SA6500.

### Instant Virtual System License (Optional)

Juniper Networks Instant Virtual System (IVS) option is designed to enable administrators to provision logically independent SSL VPN gateways within a single appliance/cluster. This allows 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 SA Series extends programmatic support to configure and manage IVS. This enables service providers to integrate IVS management into their own operations support systems (OSS). It also enables enterprises that use Instant Virtual Systems to leverage XML import/export capabilities for management of the individual virtual systems.

The IVS upgrade is available for the SA4500 and SA6500.

### High Availability License (Optional)

Juniper Networks has designed a variety of HA clustering options to support the SA Series, 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 SA2500 and SA4500 can be purchased in cluster pairs, and the SA6500 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 SA Series appliance with one or more additional SA Series appliances (depending on the platform in question). These are not additive to the concurrent user licenses. For example, if a customer has a 100 user license for the SA4500 and then purchases another SA4500 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 SA2500, SA4500, and SA6500.

### 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 SA Series 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 an SA Series 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 SA4500 and the SA6500 and includes the following features:

- Baseline
- Secure Meeting

#### Antimalware Support with Enhanced Endpoint Security (EES) (Optional)

The amount of newly discovered malicious programs that can harm endpoint devices such as PCs continues to grow. According to the 1985-2008 AV-test.org report, there were over seven million new malware programs discovered in 2008, and just over five million were discovered in 2007. Malware is known to cost enterprises an increasing amount of money every year in terms of efforts involved to quarantine and remediate appropriate endpoints.

In order to prevent endpoints from being infected with malware, Juniper Networks offers the Enhanced Endpoint Security license option. This license is a full-featured, dynamically deployable antimalware module that is an OEM of Webroot's industry-leading Spy Sweeper product. This dynamic antimalware download capability is also available with Unified Access Control. With this new capability, organizations can ensure that unmanaged and managed

Microsoft Windows endpoint devices conform to corporate security policies before they are allowed access to the network, applications, and resources. For example, potentially harmful keyloggers can be found and removed from an endpoint device before the user enters sensitive information such as their user credentials. The Enhanced Endpoint Security license protects endpoints from infection in real-time and ensures only clean endpoints are granted access to the network. Enhanced Endpoint Security licenses are available as 1-year, 2-year, and 3-year subscription options (see the Ordering Information section for more details).

The Enhanced Endpoint Security option is available for the SA2500, SA4500, and SA6500.

#### Premier Java RDP Applet (Optional)

Until now, client access software for Microsoft's Terminal Server has been cut-and-dried. Microsoft's Terminal Services client is restricted and can only be used on Windows clients with MS Internet Explorer. With the Premier Java RDP Applet option, users can remotely access centralized Windows applications independently of the client platform (Mac, Linux, Windows, and so on) through Java-based technology.

As a platform-independent solution, the Premier Java RDP Applet lets you use the entire range of Windows applications running on the Windows Terminal Server, regardless of how the client computer is equipped. By centrally installing and managing all the Windows applications, you can significantly reduce your total cost of ownership. The Premier Java RDP Applet is an OEM of the HOblink JWT (Java Windows Terminal) product created by HOB Inc., a leading European software company specializing in Java programming.

The Premier Java RDP option is available for the SA2500, SA4500, and SA6500.



## Specifications

	SA2500	SA4500	SA6500
<b>Dimensions and Power</b>			
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 W	100-240 VAC, 50-60 Hz, 2.5 A Max, 300 W	100-240 VAC, 50-60 Hz, 2.5 A Max, 400 W
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
MTBF	75,000 hours	72,000 hours	98,000 hours
Fans	Three 40 mm ball bearing fans, one 40 mm ball bearing fan in power supply	Three 40 mm ball bearing fans, one 40 mm ball bearing fan in power supply	Two 80 mm hot swap, one 40 mm ball bearing fan in power supply
<b>Panel Display</b>			
Power LED, HD activity, HW alert	Yes	Yes	Yes
HD activity and fail LED on drive tray	No	No	Yes
<b>Ports</b>			
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); for link redundancy to internal switches 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 RJ-45 serial console port
<b>Environment</b>			
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 (3,048 m) maximum	10,000 ft (3,048 m) maximum	10,000 ft (3,048 m) maximum
Altitude (storage)	40,000 ft (12,192 m) maximum	40,000 ft (12,192 m) maximum	40,000 ft (12,192 m) maximum
<b>Certifications</b>			
Common Criteria EAL3+ certification	Yes	Yes	Yes
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

## Juniper Networks Services and Support

Juniper Networks is the leader in performance-enabling services and support, which are designed to accelerate, extend, and optimize your high-performance network. Our services allow you to bring revenue-generating capabilities online faster so you can realize bigger productivity gains and faster rollouts of new business models and ventures. At the same time, Juniper Networks ensures operational excellence by optimizing your network to maintain required levels of performance, reliability, and availability. For more details, please visit [www.juniper.net/us/en/products-services/](http://www.juniper.net/us/en/products-services/).

## Ordering Information

MODEL NUMBER	DESCRIPTION
--------------	-------------

### SA2500

#### Base System

SA2500	SA2500 Base System
--------	--------------------

#### User Licenses

SA2500-ADD-10U	Add 10 simultaneous users to SA2500
SA2500-ADD-25U	Add 25 simultaneous users to SA2500
SA2500-ADD-50U	Add 50 simultaneous users to SA2500
SA2500-ADD-100U	Add 100 simultaneous users to SA2500

#### Feature Licenses

SA2500-MTG	Secure Meeting for SA2500
------------	---------------------------

#### Clustering Licenses

SA2500-CL-10U	Clustering: Allow 10 users to be shared from another SA2500
SA2500-CL-25U	Clustering: Allow 25 users to be shared from another SA2500
SA2500-CL-50U	Clustering: Allow 50 users to be shared from another SA2500
SA2500-CL-100U	Clustering: Allow 100 users to be shared from another SA2500

### SA4500

#### Base System

SA4500	SA4500 Base System
--------	--------------------

#### User Licenses

SA4500-ADD-50U	Add 50 simultaneous users to SA4500
SA4500-ADD-100U	Add 100 simultaneous users to SA4500
SA4500-ADD-250U	Add 250 simultaneous users to SA4500
SA4500-ADD-500U	Add 500 simultaneous users to SA4500
SA4500-ADD-1,000U	Add 1,000 simultaneous users to SA4500

#### Feature Licenses

SA4500-MTG	Secure Meeting for SA4500
SA4500-IVS	Instant Virtual System for SA4500
SA4500-ICE	In Case of Emergency License for SA4500
SA4500-ICE-CL	In Case of Emergency Clustering License for SA4500

#### Clustering Licenses

SA4500-CL-50U	Clustering: Allow 50 users to be shared from another SA4500
SA4500-CL-100U	Clustering: Allow 100 users to be shared from another SA2500
SA4500-CL-250U	Clustering: Allow 250 users to be shared from another SA4500
SA4500-CL-500U	Clustering: Allow 500 users to be shared from another SA4500

MODEL NUMBER	DESCRIPTION
--------------	-------------

### SA6500

#### Base System

SA6500	SA6500 Base System
--------	--------------------

#### User Licenses

SA6500-ADD-100U	Add 100 simultaneous users to SA6500
SA6500-ADD-250U	Add 250 simultaneous users to SA6500
SA6500-ADD-500U	Add 500 simultaneous users to SA6500
SA6500-ADD-1,000U	Add 1,000 simultaneous users to SA6500
SA6500-ADD-2,500U	Add 2,500 simultaneous users to SA6500
SA6500-ADD-5,000U	Add 5,000 simultaneous users to SA6500
SA6500-ADD-7,500U	Add 7,500 simultaneous users to SA6500
SA6500-ADD-10,000U	Add 10,000 simultaneous users to SA6500
SA6500-ADD-12,500U*	Add 12,500 simultaneous users to SA6500
SA6500-ADD-15,000U*	Add 15,000 simultaneous users to SA6500
SA6500-ADD-20,000U*	Add 20,000 simultaneous users to SA6500
SA6500-ADD-25,000U*	Add 25,000 simultaneous users to SA6500

#### Feature Licenses

SA6500-MTG	Secure Meeting for SA6500
SA6500-IVS	Instant Virtual System for SA6500
SA6500-ICE	In Case of Emergency License for SA6500
SA6500-ICE-CL	In Case of Emergency Clustering License for SA6500

#### Clustering Licenses

SA6500-CL-100U	Clustering: Allow 100 users to be shared from another SA6500
SA6500-CL-250U	Clustering: Allow 250 users to be shared from another SA6500
SA6500-CL-500U	Clustering: Allow 500 users to be shared from another SA6500
SA6500-CL-1000U	Clustering: Allow 1,000 users to be shared from another SA6500
SA6500-CL-2500U	Clustering: Allow 2,500 users to be shared from another SA6500
SA6500-CL-5000U	Clustering: Allow 5,000 users to be shared from another SA6500
SA6500-CL-7500U	Clustering: Allow 7,500 users to be shared from another SA6500
SA6500-CL-10000U	Clustering: Allow 10,000 users to be shared from another SA6500
SA6500-CL-12500U	Clustering: Allow 12,500 users to be shared from another SA6500
SA6500-CL-15000U	Clustering: Allow 15,000 users to be shared from another SA6500
SA6500-CL-20000U	Clustering: Allow 20,000 users to be shared from another SA6500
SA6500-CL-25000U	Clustering: Allow 25,000 users to be shared from another SA6500

\*Multiple SA6500s required



## Ordering Information (continued)

MODEL NUMBER	DESCRIPTION
<b>Accessories</b>	
UNIV-CRYPTO	Field upgradeable SSL acceleration module for SA4500
UNIV-PS-400W-AC	Field upgradeable secondary 400 W power supply for SA6500
UNIV-80G-HDD	Field replaceable 80 GB hard disk for SA6500
UNIV-MR2U-FAN	Field replaceable fan for SA6500
UNIV-MRIU-RAILKIT	Rack mount kit for SA2500 and SA4500
UNIV-MR2U-RAILKIT	Rack mount kit for SA6500
UNIV-SFP-FSX	Mini-GBIC transceiver - fiber SX for SA6500
UNIV-SFP-FLX	Mini-GBIC transceiver - fiber LX for SA6500
UNIV-SFP-COP	Mini-GBIC transceiver - copper for SA6500
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](http://www.juniper.net).

### Corporate and Sales Headquarters

Juniper Networks, Inc.  
1194 North Mathilda Avenue  
Sunnyvale, CA 94089 USA  
Phone: 888.JUNIPER (888.586.4737)  
or 408.745.2000  
Fax: 408.745.2100  
[www.juniper.net](http://www.juniper.net)

### APAC Headquarters

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

### EMEA Headquarters

Juniper Networks Ireland  
Airside Business Park  
Swords, County Dublin, Ireland  
Phone: 35.31.8903.600  
EMEA Sales: 00800.4586.4737  
Fax: 35.31.8903.601

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

Copyright 2010 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, Junos, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.