SA SERIES SSL VPN APPLIANCES

SA2500, SA4500, SA6500

Product Overview

Juniper Networks SA Series SSL VPN Appliances provide a complete range of remote access appliances for all size companies, as well as Juniper Networks SA Series SSL VPN Virtual Appliances (see separate datasheet). The SA Series includes Juniper Networks Junos Pulse, which provides a simple, intuitive enabling user interface that provides secure, authenticated access for mobile and remote users from any web-enabled device The SA Series combines the security of SSL with standards-based access controls, granular policy creation, and unparalleled flexibility. The result is ubiquitous security for all enterprise tasks, with options for increasingly stringent access control to protect the most sensitive applications and data, and deliver lower total cost of ownership over traditional IPsec client solutions.

Product Description

The Juniper Networks® SA2500, SA4500, and SA6500 SSL VPN Appliances meet the needs of companies of all sizes. 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. The 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 includes Juniper Networks Junos® Pulse, a dynamic, integrated, multiservice network interface for mobile and nonmobile devices. Junos Pulse enables optimized, accelerated, anytime, anywhere access to corporate networks, clouds, and the data they hold. Junos Pulse enables secure SSL access from a wide range of mobile and nonmobile devices, including smartphones, tablets, laptops, and desktop PCs, as well as Wi-Fi or 3G/4G and Long Term Evolution (LTE)-enabled devices. Junos Pulse delivers enterprises improved productivity and secure, ubiquitous access to corporate applications and data—anytime, anywhere.

Architecture and Key Components

The SA2500 SSL VPN Appliance enables small to medium-sized businesses (SMBs) to deploy granular, cost-effective mobile and remote network and cloud access, as well as intranet security and business continuity in case of disaster or emergency. Users can access the corporate resources and applications from any endpoint device 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-sized organizations to provide efficient, role-based corporate network, cloud, and application access to mobile and remote employees, as well as authorized contractors and partners, requiring only a Web browser connected to the Internet. The SA4500 features rich access privilege management functionality that can be used to create secure customer/partner extranets and to enable secure access to the corporate intranet, so that employees and other authorized users can use the same access means but with differentiated, role-based access while still adhering to enterprise security policies. Built-in compression for all traffic types speeds performance, and 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 encryption/decryption processes.

Because each of the SA Series SSL VPN Appliances runs the same software, there is no need to compromise user or administrator experience based on which appliance you choose. All devices offer leading performance, stability, and scalability. Therefore, deciding which device best fits 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 mobile and 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-sized to large-sized 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 who 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.

Features and Benefits

Junos Pulse

Junos Pulse is an integrated, multiservice network interface enabling anytime, anywhere connectivity and access, security, network access control, acceleration, and collaboration 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 nonmobile, Wi-Fi or 3G/4G/LTE-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	• Layer 3 VPN connectivity with granular access control is provided. • Supports SSL mode or Encapsulating Security Payload (ESP) transport mode.
Ease of use	• Seamless roaming from remote access (to SA Series) to local LAN access (via Juniper Networks Unified Access Control) is provided for laptops. • Junos Pulse can be preconfigured by administrators to automatically prompt end users for credentials to authenticate to the SA Series when they are remote.
Endpoint security	• Full Host Checker capability enables endpoint security to be checked for Windows, Mac OS, and Linux devices as well as Apple iOS and Google Android mobile devices. Host Checker for iOS and Android platforms enables administrators to restrict or prohibit VPN access from noncompliant devices based on centrally defined corporate policies, including mobile OS version restrictions, jail-broken or rooted status, or presence and/or enablement of Junos Pulse Mobile Security Suite.
Split tunneling options (enable or disable with overriding route capability and route monitoring)	• Key split tunneling options are supported. • Secure, granular access control is enforced.
Flexible launch options (standalone client, browser-based launch)	• Users can easily launch Junos Pulse via the Web from the SA Series landing page. • Remote users can simply launch Junos Pulse from their desktop or mobile device.
Preconfiguration options (preconfigured installer to contain list of SA Series appliances)	• For laptops and desktop PCs, administrators can preconfigure a Junos Pulse deployment with a list of corporate SA Series appliances for end users to choose from.
Connectivity options (max/idle session timeouts, automatic reconnect, logging)	• Administrators can set up flexible connectivity options for remote users.
Authentication options (hardware token, smart cards, or soft token)	• Administrators can deploy Junos Pulse for remote user authentication by using a hardware token or smart cards. • Junos Pulse supports integration with RSA SoftID, allowing automatic access to the user's RSA passcodes using the PIN entered by the user.

For more details on Junos Pulse, please visit **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 device: Supports up to 10,000 concurrent users
- Two-unit cluster of SA6500 devices: Supports up to 18,000 concurrent users
- Three-unit cluster of SA6500 devices: Supports up to 26,000 concurrent users
- Four-unit cluster of SA6500 devices: 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
Patch auto-remediation (optional)	Automatically remediates noncompliant endpoints by updating software applications that do not comply to corporate security policies. Does not require Microsoft SMS protocol for remediation and covers patches for not only Microsoft but other vendors such as Adobe, Firefox, Apache, RealPlayer, etc. Directly downloads missing patches from vendor's website without going through the SA Series appliance.	Improves productivity of remote users by enabling them to gain immediate access to the corporate network without having to wait for periodic updates of software applications. Ensures compliance with corporate security policies.
Host Checker for client computers	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). Host Checker 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 and quarantining devices when necessary. Ensures that no potentially sensitive data is left behind on the endpoint device.
Host Checker for mobile devices	Host Checker support for mobile devices running the Apple iOS or Google Android operating systems allows administrators to restrict or prohibit VPN access from noncompliant devices based on corporate-defined security policies.	Secures mobile remote network, cloud, and application access via SSL VPN for iOS and Android devices based on the integrity of the device and mobile OS.
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 noncompliant devices. For mobile devices, Host Checker can enforce policies based on mobile OS version, jail-broken/rooted status, and/or status of the Junos Pulse Mobile Security Suite on the device (installed/not installed, active/inactive).	Uses current security policies with remote users and devices; provides easier management.
Trusted Network Connect (TNC) support on Host Checker	Allows standards-based 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 who run other security clients.	Enables access to extranet endpoint devices such as PCs from partners that might 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.

Ease of Administration

In addition to enterprise-class security benefits, the SA2500, SA4500, and SA6500 appliances 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 certificate authority (CA) support	Enables the SA Series to support federated public key infrastructure (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 according to 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—there are no APIs for directory integration, as they are all native/built in.
Integration with strong authentication and identity and access management (IAM) platforms	Provides ability to support SecurID; Security Assertion Markup Language (SAML), including standards-based SAML v2.0 support, and PKI/digital certificates. Includes SAML 2.0 support for web/cloud single sign-on (SSO).	Leverages existing corporate authentication methods to simplify administration, and allows enterprises to easily and securely federate user identity with Software-as-a-Service (SaaS) and other cloud-based applications.
Multiple hostname support	Provides the ability to host different virtual extranet websites from a single SA Series appliance.	Saves the cost of incremental servers, eases management overhead, and provides a transparent user experience with differentiated entry URLs.
Customizable user interface	Allows for creation of completely customized sign-on pages, including customized landing pages for tablets.	Provides an individualized look for specified roles, streamlining the user experience.
Juniper Networks Network and Security Manager (NSM)	Provides 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) (option)	Provides licenses for a large number of additional users on an SA Series 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	Provides the ability for any platform to gain access to resources such as Windows, Mac OS, Linux, or mobile devices running various mobile operating systems, including Apple iOS, Google Android, Microsoft Windows Mobile, Nokia Symbian, and RIM Blackberry.	Provides flexibility in allowing users to access corporate resources from virtually any type of device using virtually any type of OS.
Enterprise licensing	Allows any organization with one or more devices to easily lease licenses from one appliance to another as required to adapt to changing organizational needs.	Provides administrators the ability to start with minimal per-device licensing costs and then incrementally upgrade to enterprise leased licensing capabilities as needed.

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 in to the SA Series SSL VPN Appliances, 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 the end user experience.
Certificate authentication to backend servers	Enables customers to enforce client authentication on their secure backend servers, and allows the SA Series to present an administrator-configured certificate to these servers for authentication.	Allows customers to mandate strict SSL policies on their backend servers by configuring client authentication.
Client certificate authentication 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 standalone (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.
Virtual Desktop Infrastructure (VDI) support	Allows interoperability with VMware View Manager 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 servers. Provides dynamic delivery of 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 mobile devices running Symbian, Windows Mobile, iOS, or Android) to the Exchange server with no client software installation. Enables up to 5,000 simultaneous sessions on the SA6500.	Enables customers to allow a large number of users—including employees, and authorized contractors and partners—to access corporate resources through mobile devices via ActiveSync.
Mobile-friendly SSL VPN login pages	Provides predefined HTML pages that are customized for mobile devices, including Apple iPhones and iPad, Google Android, and other mobile devices.	Provides mobile device users with a simplified and enhanced user experience with Web pages customized to their device types.
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. Customized variables as well as FASC-N attributes are supported.	Enables the administrator to provision by purpose for each unique session.
Resource authorization	Provides extremely granular, differentiated access control to the URL, server, or file level for users based on their different roles.	Allows administrators to tailor security policies to specific groups and user roles, providing authorized access only to essential data.
Granular auditing and logging	Can be configured to the per-user, per-resource, and 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. Suitable for regulatory compliance and associated audits.

Flexible Single Sign-On (SSO) Capabilities

The SA2500, SA4500, and SA6500 offer comprehensive SSO features. These features increase end user productivity and quality of experience, 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	Provides support for Kerberos Constrained Delegation protocol. When a user logs in to the SA Series with a credential that cannot be proxied through to the backend server, the SA Series appliance retrieves a Kerberos ticket on behalf of the user from the Active Directory infrastructure. The ticket is cached on the SA Series appliance throughout the session. When the user accesses Kerberos-protected applications, the SA Series uses 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.

Table 4: Flexible Single Sign-on Features and Benefits (continued)

Feature	Feature Description	Benefits
Kerberos SSO and NTLMv2 support	The SA Series automatically authenticates remote users via Kerberos or NTLMv2 by using user credentials.	Simplifies user experience by avoiding having users enter credentials multiple times to access different applications.
Password management integration	Provides a 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. The users can manage their passwords directly through the SA Series interface.
Web-based 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 reentering 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	Provides ability to pass username, credentials, and other customer-defined and customizable attributes to the authentication forms of other products and as header variables.	Enhances user productivity and provides a customized experience.
SAML 2.0 support for Web/ cloud SSO	Acts as a SAML IdP (Identity Provider) for service provider initiated SSO to enable simple and transparent access to cloud-based applications for remote users. Leverages Junos Pulse or Network Connect for SSO for web-based applications.	Seamless and transparent SSO for cloud/web-based applications enhances remote user experience and productivity. Extends proven and secure authentication to cloud-based SaaS applications and other Web applications.

Provision by Purpose

The SA2500, SA4500, and SA6500 SSL VPN Appliances 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 tablets, mobile devices, and smartphones, which support IKEv2 VPN connectivity. Administrators can also enable strict certificate authentication for access via IPsec/IKEv2. Also enables username/password authentication through Extensible Authentication Payload (EAP), whereby IKEv2 provides a "tunnel" mechanism for EAP authentication.	· Extends Juniper's leading mobility and access control features of the SA Series to a 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	Provides 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 such as Outlook Web Access (OWA), Windows and UNIX file share, telnet/SSH hosted applications, terminal emulation, SharePoint (including extensive SharePoint 2010 support), and others.	· Provides the most easily accessible form of application and resource access from a variety of end user devices, including mobile devices. · Enables extremely granular security control options. · Offers a completely clientless approach using only a Web browser.
Secure Application Manager (SAM)	A lightweight Java or Windows-based download enables 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 preinstalled client.
Network Connect (NC)	Provides complete network-layer connectivity via an automatically provisioned cross-platform download; Windows Logon/GINA integration for domain SSO; and installer services to mitigate need for administrator rights. Allows for split tunneling capability.	· Users only need a Web browser. · NC 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 administrator 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	This single, integrated remote access enabling interface can also provide LAN access control, application acceleration, online meeting and collaboration services, and dynamic VPN features to remote users, in conjunction with Juniper Networks MAG Series Junos Pulse Gateways running Junos Pulse services, including Junos Pulse Access Control Service or Junos Pulse Application Acceleration Service; or Juniper Networks Unified Access Control and SRX Series Services Gateways devices.	· Junos Pulse replaces the need to deploy and maintain multiple, separate clients for different functionalities such as VPN, network (LAN) access control, application acceleration, and online meeting/collaboration services. · By seamlessly integrating all of these functionalities into one single, easy-to-use, multiservice enabling interface, working across multiple computing and mobile operating platforms, administrators can save on client management, training, and deployment costs to end users.

Product Options

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

User License (Common Access 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.

With SSL VPN 7.1 software (or later), common access licenses are now available as user licenses. With common access licensing, user licenses can either be used for SA Series user sessions or Juniper Networks IC Series Unified Access Control Appliances user sessions. This simplifies the licensing model that can be used across SA Series and UAC models. Please see the "Ordering Information" section for the common access license SKUs that can be used for the SA Series or for the UAC models going forward.

User licenses provide the functionality that allows the mobile, remote, and intranet user to access the network, cloud, and their resources. They fully meet the needs of both basic and complex deployments with diverse audiences and use cases, and they require little or no client software, server changes, DMZ build-outs, or software client 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 now allows for up to 200 concurrent users.

Key features enabled by this license include:

- Junos Pulse, Secure Application Manager, and Network Connect provide cross-platform support for client/server applications using SAM, as well as full network-layer access using either the ESP or SSL transport mode of Junos Pulse, along with the adaptive dual transport methods of Network Connect. The combination of SAM, Junos Pulse, and Network Connect with Core Clientless access provides secure access for virtually any audience, from mobile or remote workers, to partners or customers, over a wide range of devices and operating platforms, from nearly 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 login 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 device so that nothing is left behind.

High Availability Clustering

With the introduction of SSL VPN 7.0 (or later) software releases, customers now have the ability to build clusters without buying any additional licenses.

The clustering method can be explained in two simple steps

1) Simply place an equal number of user ("-ADD") licenses on each box.
2) When they are joined together to form a cluster, all of the user licenses add up so that the cluster can now support all of the licensed users. For example, building a 1,000-user cluster is done by bringing together two boxes with 500 user licenses in each of the two units.

Clustering allows 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, this provides a total of 100 users that are shared across both appliances, not per appliance.

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. Clustering also provides 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, so in the unlikely event that one unit fails, system configurations (such as authentication server, authorization groups, and bookmarks), user profile settings (such as 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.

HA capability is available for the SA2500, SA4500, and SA6500.

In Case of Emergency (ICE) License (Optional)

SSL VPNs can help keep organizations and businesses functioning securely 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 Juniper Networks SA Series ICE license delivers a timely solution for addressing a dramatic peak in demand for mobile or remote access to ensure business continuity whenever a disastrous event strikes. ICE licenses provide for a large number of additional users on an SA Series appliance for a limited time. With ICE licenses, businesses can:

- Maintain productivity by enabling ubiquitous access to applications and information for employees from anywhere, at any time, and from virtually any device—desktop PCs, kiosks, laptops, smartphones, tablets, etc.
- Sustain partnerships with around-the-clock, real-time access to applications and services while knowing that resources are secured and protected.
- Continue to deliver exceptional service to customers and partners via 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 Baseline features.

Premier Java RDP Applet (Optional)

With the Premier Java RDP Applet option, users can remotely access centralized Windows applications independent of the client platform (Mac OS, Linux, Windows, etc.) 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 of 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 Applet option is available for the SA2500, SA4500, and SA6500

SA6500

SA2500

SA4500

Specifications

	SA2500	SA4500	SA6500
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, 1 U	Yes, 1 U	Yes, 2 U, 19 in
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 in) cold-rolled steel	18 gauge (.048 in) 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
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); 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

Environment

- Operating temp: 41º to 104º F (5º to 40º C)
- Storage temp: -40º to 158º F (-40º to 70º C)
- Relative humidity (operating): 8% to 90% noncondensing
- Relative humidity (storage): 5% to 95% noncondensing
- Altitude (operating): 10,000 ft (3,048 m) maximum
- Altitude (storage): 40,000 ft (12,192 m) maximum

Certifications

- Common Criteria EAL3+ certification
- Safety certifications: 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
- Warranty: 90 days; can be extended with support contract

Juniper Networks Services and Support

Juniper Networks is the leader in performance-enabling services that are designed to accelerate, extend, and optimize your high-performance network. Our services allow you to maximize operational efficiency while reducing costs and minimizing risk, achieving a faster time to value for your network. Juniper Networks ensures operational excellence by optimizing the network to maintain required levels of performance, reliability, and availability. For more details, please visit **www.juniper.net/us/en/products-services**.

Ordering Information

Model Number	Description
Base Systems	
SA2500	SA2500 Base System
SA4500	SA4500 Base System
SA6500	SA6500 Base System
Accessories	
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-MR1U-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
User Licenses (Common Access Licensing)	
ACCESSX500-ADD-xU	Add x simultaneous users to SA Series or ICX500 Series appliances (x options: 10, 25, 50, 100, 250, 500, 1000, 2000, 2500, 5000 or 10K, simultaneous users)
High Scale Licenses (Common Access Licensing)	
ACCESSX500-ADD-xU	Add x simultaneous users to SA Series or ICX500 Series appliances (x options: 15K*, 20K*, or 25K* simultaneous users)

*Multiple SA6500s required

Model Number	Description
Feature Licenses	
SA4500-ICE	In Case of Emergency License for SA4500
SA4500-ICE-CL	In Case of Emergency Clustering License for SA4500
SA6500-ICE	In Case of Emergency License for SA6500
SA6500-ICE-CL	In Case of Emergency Clustering License for SA6500
Java RDP Applet Licenses	
ACCESS-RDP-xU-zYR	Java RDP Applet z-Year subscription for x simultaneous users (x options: 50, 100, 250, 500, 1000, 2000, 2500, 5000, 7500, or 10K simultaneous users. RDP user license count cannot exceed the number of user licenses/common access licenses) (z options: 1, 2, or 3 year subscription)

About Juniper Networks

Juniper Networks is in the business of network innovation. From devices to data centers, from consumers to cloud providers, Juniper Networks delivers the software, silicon and systems that transform the experience and economics of networking. The company serves customers and partners worldwide. Additional information can be found at **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

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.

1000220-014-EN Nov 2012

Printed on recycled paper