



SA4500 FIPS AND SA6500 FIPS SSL VPN APPLIANCES

Product Overview

Government agencies and their IT staff are chartered with reconciling seemingly opposing goals: provide reliable and timely information access to government employees and citizens while protecting sensitive resources. Federal agencies are further directed to procure only those IT technologies that have been certified to meet the rigors of government communication standards. While required for government agencies, these strictures also provide useful guidelines to private sector businesses that require stringent security. Juniper Networks SA4500 FIPS and SA6500 FIPS SSL VPN Appliances uniquely delivers on these needs by providing the most flexible, secure, field hardened access available among U.S. government-certified solutions.

Product Description

Juniper Networks is the market leader in SSL-based remote access that is easy to deploy and easy to maintain. All Juniper Networks® SA Series SSL VPN Appliances have met or exceeded the stringent security standards of independent Internet security auditing agencies. Juniper extends this leadership with a FIPS-certified hardware security module that is Federal Information Processing Standards (FIPS) compliant. Like all SA Series appliances, the Juniper Networks SA4500 FIPS SSL VPN Appliance and SA6500 FIPS SSL VPN Appliance provide a hardened security gateway that uses standards-based SSL protocol to provide remote access via a Web browser. There are no hardware or software clients to deploy, configure, or install; no changes required for internal servers; no Network Address Translation (NAT) or firewall traversal issues to manage; and virtually no ongoing maintenance. SSL is the most widely deployed security protocol in the world, securing billions of dollars in online banking and e-commerce transactions. The combination of these features adds up to a solution with unbeatable security, radically lower total cost of ownership (TCO) when compared to traditional VPNs or custom extranets, and a highly scalable implementation.

Architecture and Key Components

The SA4500 FIPS and SA6500 FIPS appliances offer numerous capabilities to address government agencies stringent security requirements while enabling access for their employees and users in a timely fashion. The following section lists the capabilities.

FIPS Security

- Stringent security with FIPS-certified Hardware Security Module (HSM) and FIPS-certified Layer 3 connectivity using the Network Connect client on Windows platform.

Provision by Purpose

- Different access methods that allow administrators to balance security and access on a per-user, per-session basis

Rich access privilege management capabilities

- Dynamic, controlled access at the URL, file, application, and server level based on a variety of session-specific variables, including identity, device, security control, and network trust level

End-to-End Layered Security

- Numerous security options from the end user device to the application data and servers, including coordinated threat control with Juniper Networks IDP Series Intrusion Detection and Prevention Appliances
- Native functionality, client- and server-side APIs, and advanced malware protection for effective enforcement and unified administration of best-in-class endpoint security

Ease of administration

- Central management option for unified administration
- User self-service features that enhance productivity while lowering administrative overhead

Flexible single sign-on (SSO) capabilities

- Comprehensive SSO features to increase end user productivity, greatly simplify administration of large diverse user resources, and significantly reduce the number of help desk calls

Performance scalability with SA6500 FIPS

- A variety of performance enhancing features, including a hardware-based SSL acceleration module and clustering to provide optimal scalability
- Up to 3,500 concurrent users supported on a single unit, and up to 10,000 concurrent users supported on a four unit cluster

- Dual hot-swappable hard drives, dual hot-swappable fans
- Hot-swappable power supplies (second power supply optional, DC power supplies available)
- 4 GB SDRAM
- 4-port copper 10/100/1000 interface card, and a 1-port copper 10/100/1000 management interface

High Availability (HA)

- Cluster pair deployment option for high availability (HA) across the LAN

Features and Benefits

FIPS Security

The SA4500 FIPS and SA6500 FIPS appliances incorporate a FIPS-certified HSM. The HSM handles cryptographic processing as well as key and certificate management in a hardened, tamper-proof hardware module. The HSM provides the additional benefit of offloading cryptographic processing from the host CPU, thus optimizing overall system performance while adding a physical layer of security. The SA4500 FIPS and SA6500 FIPS appliances also have a tamper evident label that deters physical security breaches and provides visual indication of appliance integrity.

Table 1: Security

FEATURE	FEATURE DESCRIPTION	BENEFIT
FIPS140-2 Level 3 certified for the HSM and Network Connect client	<ul style="list-style-type: none">• Complies with the latest U.S. Government best practices.• FIPS140-2 is recognized by CESG as meeting security criteria for use in data traffic categorized as "Private." (CESG is the UK Government's National Technical Authority for Information Assurance, responsible for enabling secure and trusted knowledge.)	Advanced protection to provide the most stringent security.

Provision by Purpose

The SA4500 FIPS and SA6500 FIPS appliances include three different access methods. These different methods are selected as part of the user's role, allowing the administrator to enable the appropriate access on a per-session basis, taking into account user, device, and network attributes in combination with enterprise security policies.

Table 2: Provision by Purpose

FEATURE	FEATURE DESCRIPTION	BENEFIT
IPsec/IKEv2 support for mobile devices	Allows remote users to connect from devices such as PDAs, mobile devices, and smartphones that support Internet Key Exchange (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.	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 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	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 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 Installation and Configuration 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.

Access Privilege Management Capabilities

The SA4500 FIPS and SA6500 FIPS appliances 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 an SA4500 FIPS or SA6500 FIPS appliance, they pass through a pre-authentication assessment, and are then dynamically mapped to the session role that combines established network, device, identity, and session policy settings. Granular resource authorization policies further ensure exact compliance to security strictures.

Table 3: Access Privilege Management Capabilities

FEATURE	FEATURE DESCRIPTION	BENEFIT
UAC/SA Series 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 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 admin 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 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 and Citrix XenDesktop to enable administrators to deploy virtual desktops with the SA Series appliances.	Provides seamless remote user access to 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 5,000 simultaneous sessions on the SA6500.	Simplifies the end user experience when using a mobile device to get network access.
Mobile-friendly SSL VPN login pages	Provides predefined HTML pages that are customized for mobile devices, including Apple iPhone and iPad, Google Android, and Nokia Symbian devices.	Provides mobile device users with a simplified and enhanced user experience, with webpages customized for 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.	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 at 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.

End-to-End Layered Security

The SA4500 FIPS and SA6500 FIPS appliances provide complete, end-to-end layered security, including endpoint client, device, data, and server layered security controls. These include:

Table 4: End-to-End Layered Security

FEATURE	FEATURE DESCRIPTION	BENEFIT
Antispyware support with Enhanced Endpoint Security (EES)	Dynamically download Webroot's market-leading anti-malware 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 spyware, protecting corporate resources from harm during network access. Enables dynamic enforcement of anti-malware protection on unmanaged assets such as PCs of external partners, customers, or suppliers.
Endpoint auto-remediation	Automatically remediates noncompliant endpoints by updating software applications that do not comply with corporate security policies. Does not require Microsoft's short message service (SMS) protocol for remediation, and covers patches for not only Microsoft, but other vendors such as Adobe, Firefox, Apache, RealPlayer, and so on. Directly downloads missing patches from vendor's website without going through the SA Series appliance.	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 security posture requiring installed/running endpoint security applications (antivirus, firewall, other). Also supports custom-built checks such as verifying ports opened/closed, checking files/processes and validating their authenticity with Message Digest 5 (MD5) hash checksums, verifying registry settings, machine certifications, and more. Includes cache cleaner that erases all proxy downloads and temp files at logout.	Verifies/ensures that each endpoint device meets corporate security policy requirements before granting access, remediating devices and quarantining users when necessary. Also, ensures that 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 noncompliant endpoints.	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 hosts that are not API-compliant 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 who may run security clients which are different from 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 back doors to exploit or hack.
Security services that 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 unsecure kiosks after a session.
Coordinated threat control	Enables SA Series and IDP Series 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

The SA4500 FIPS and SA6500 FIPS appliances have a wealth of features that make them easy for the administrator to deploy and manage.

Table 5: Ease of Administration

FEATURE	FEATURE DESCRIPTION	BENEFIT
Bridge certificate authority (CA) 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). It also enables the customer to configure policy extensions in the SA Series admin UI to enforce policies 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, identity, and access management platforms	Provides ability to support RSA SecurID; Security Assertion Markup Language (SAML), including standards-based SAML v2.0 support, and PKI/digital certificates.	Leverages existing corporate authentication methods to simplify administration.
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.	Provides an individualized look for specified roles, streamlining the user experience.
Juniper Networks Network and Security Manager	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)	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, 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 OS.
Enterprise licensing	Allows any organization with one or more devices to easily lease licenses from one appliance to another to adapt to changing organizational needs, as required.	Provides administrators the ability to start with minimal per-device licensing costs and then incrementally upgrade to enterprise leased licensing capabilities as needed.

Flexible Single Sign-On (SSO) Capabilities

The SA4500 FIPS and SA6500 FIPS offer comprehensive SSO 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 6: Flexible SSO Features and Benefits

FEATURE	FEATURE DESCRIPTION	BENEFIT
Kerberos Constrained Delegation	Provides 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 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 6: Flexible SSO Features and Benefits (continued)

FEATURE	FEATURE DESCRIPTION	BENEFIT
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).	Leverages 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 attributes to the authentication forms of other products and as header variables.	Enhances user productivity and provides a customized experience.

Performance Scalability with the SA6500 FIPS

SA6500 FIPS is specifically designed to accommodate large numbers of users with complex application needs, and provides application performance optimization via compression algorithms and hardware-based SSL acceleration. These features allow the appliance to process large, simultaneous transaction loads while minimizing perceptible latency to users.

Table 7: SA6500 FIPS Performance Scalability

FEATURE	FEATURE DESCRIPTION	BENEFIT
Built-in, hardware-based SSL acceleration	Offloads compute intensive encrypt/decrypt process from the CPU.	Enhanced performance.
Optional 4-port small form-factor pluggable (SFP) interface card with flexibility to select SX, LX, and copper-based Gigabit Interface Connector (GBIC) interfaces	Fully redundant/meshed configuration of SSL VPN appliances with multiple load balancers.	Optimized uptime.
4-port copper 10/100/1000 interface card	Provides high-speed Gigabit Ethernet connections to internal switches.	Enables link redundancy to the LAN.
Clustering	Cluster pairs or multiunit clusters can be deployed across the LAN for superlative scalability with a large number of user licenses.	Access scales as the user base grows.

High Availability

The SA4500 FIPS and SA6500 FIPS appliances include a variety of unique, “first in industry” capabilities for the availability and redundancy required for mission critical access in demanding enterprise environments. With the introduction of SA Series version 7.0 (or later) software releases, customers have the ability to build clusters without buying any additional licenses.

The clustering method can be achieved with 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. These are not additive to the concurrent user licenses. For example, if a customer has a 100-user license for the SA4500 FIPS and then purchases another SA4500 FIPS, this provides a total of 100 users that are shared across both appliances, not per appliance.

Table 8: FIPS Lower TCO

FEATURE	FEATURE DESCRIPTION	BENEFIT
SA4500 and SA6500 FIPS		
Stateful peering	Units that are part of a cluster pair synchronize system state, user profile state, and session state data among a group of appliances in the cluster.	Seamless failover with minimal user downtime and loss of productivity.
Clustering	Cluster pairs multiply aggregate throughput to handle unexpected burst traffic as well as resource intensive application use. Clusters can be deployed in either active/passive or active/active modes across the LAN	Superlative scalability with a large number of user licenses that scale access as the user base grows.
SA6500 FIPS Only		
Dual mirrored, hot-swappable, Serial Advanced Technology Attachment (SATA) hard drives; dual hot-swappable fans and hot swappable power supplies (second power supply optional, DC power supplies available)	Ensures continuous operation in the rare event of component failure.	Optimized uptime, operational convenience, high availability.

User License (Common Access Licenses)

With version 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 new common access license SKUs that can now be used for the SA Series or for the UAC models going forward.

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 they 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 is additive. For example, if a 100-user license were 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:

- SAM and Network Connect provide cross-platform support for client/server applications using SAM, as well as full network-layer access using the adaptive dual transport methods of Network Connect. The combination of SAM 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 features provide 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 (SVW) 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.

Product Options

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—along with 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.

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 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 appliance for a limited time. With ICE, businesses can do the following:

- 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 includes the following functionality:

- Baseline
- Secure Meeting

Anti-Malware Support with Enhanced Endpoint Security (EES) (Optional)

The number of newly discovered malicious programs that can harm endpoint devices such as PCs continues to grow and replicate at an alarming rate. 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 anti-malware module that is an OEM of Webroot's industry-leading Spy Sweeper product. This dynamic anti-malware 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 their network, applications, and resources. For example, potentially harmful keyloggers can be found and removed from an endpoint device before users enter sensitive information such as their user credentials. The EES license protects endpoints from infection in real time, and it ensures that 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).

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, 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 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.



SA4500 FIPS



SA6500 FIPS

Specifications

	SA4500 FIPS	SA6500 FIPS
Upgrade Options		
Software	<ul style="list-style-type: none"> Secure Meeting upgrade option In Case of Emergency (ICE) upgrade option Additional users upgrade option Enhanced Endpoint Security option 	<ul style="list-style-type: none"> Secure Meeting upgrade option In Case of Emergency (ICE) upgrade option Additional users upgrade option Enhanced Endpoint Security option
Hardware	None	<ul style="list-style-type: none"> Field upgradeable secondary 400 W power supply Field replaceable 80 gigabyte hot-swappable hard disk Field replaceable hot-swappable fan 4-port SFP GBIC transceiver <ul style="list-style-type: none"> 1000BASE-T RJ45 copper 1000BASE-SX fiber 1000BASE-LX fiber
Technical Specifications		
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 3.5 x 17.72 in (43.8 x 8.8 x 45 cm)
Weight	15.6 lb (7.1 kg) typical (unboxed)	26.4 lb (12 kg) typical (unboxed)
Material	18 gauge (.048 in) cold-rolled steel	18 gauge (.048 in) cold-rolled steel
Fans	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
Rack-mountable	19 inches, 1U	19 inches, 1U
Panel Display	<ul style="list-style-type: none"> Power LED, HD Activity, HW Alert FIPS Status LED HSM Status LED 	<ul style="list-style-type: none"> Power LED, HD Activity, HW Alert HD Activity and Fail LED on Drive Tray FIPS Status LED HSM Status LED
PS fail	No	No
HDD activity and RAID status LEDs	No	No
Ports		
Network	<ul style="list-style-type: none"> Two RJ-45 Ethernet: 10/100/1000 full or half duplex (auto-negotiation) Fast Ethernet: IEEE 802.3u compliant Gigabit Ethernet: IEEE 802.3z or IEEE 802.3ab compliant 	<ul style="list-style-type: none"> Management: One RJ-45 Ethernet – 10/100/1000 full or half-duplex (auto-negotiation) Traffic <ul style="list-style-type: none"> Four RJ-45 Ethernet – full or half-duplex (auto-negotiation); for link redundancy to internal switches SFP module optional Fast Ethernet: IEEE 802.3u compliant Gigabit Ethernet: IEEE 802.3z or IEEE 802.3ab compliant
Console	One RJ-45 serial console port	One RJ-45 serial console port
Power		
AC Power Wattage	Max, 300 W	Max, 400 W
AC Power Voltage	100-240 VAC, 50-60 Hz, 2.5 A	100-240 VAC, 50-60 Hz, 2.5 A
System Battery	CR2032 3V lithium coin cell	CR2032 3V lithium coin cell
Efficiency	80% minimum, at full load	80% minimum, at full load
Mean time between failures (MTBF)	72,000 hours	98,000 hours
Environment		
Operating temp	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)
Relative humidity (operating)	8% to 90% noncondensing	8% to 90% noncondensing
Relative humidity (storage)	5% to 90% noncondensing	5% to 90% noncondensing
Altitude (operating)	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

Specifications (continued)

	SA4500 FIPS	SA6500 FIPS
Certifications		
Common Criteria EAL3+ certification	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
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
Warranty	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.

Ordering Information

MODEL NUMBER	DESCRIPTION
SA4500 FIPS	
Base System	
SA4500FIPS	SA4500 FIPS Base System
User Licenses (Common Access Licensing)	
ACCESSX500-ADD-10U	Add 10 simultaneous users to SA Series or ICX500 Series appliances
ACCESSX500-ADD-25U	Add 25 simultaneous users to SA Series or ICX500 Series appliances
ACCESSX500-ADD-50U	Add 50 simultaneous users to SA Series or ICX500 Series appliances
ACCESSX500-ADD-100U	Add 100 simultaneous users to SA Series or ICX500 Series appliances
ACCESSX500-ADD-250U	Add 250 simultaneous users to SA Series or ICX500 Series appliances
ACCESSX500-ADD-500U	Add 500 simultaneous users to SA Series or ICX500 Series appliances
ACCESSX500-ADD-1000U	Add 1,000 simultaneous users to SA Series or ICX500 Series appliances
Feature Licenses	
SA4500-MTG	Secure Meeting for SA4500 FIPS
SA4500-IVS	Instant Virtual System for SA4500 FIPS
SA4500-ICE	In Case of Emergency License for SA4500 FIPS
SA4500-ICE-CL	In Case of Emergency Clustering License for SA4500 FIPS
Clustering Licenses	
SA4500-MTG	Secure Meeting for SA4500 FIPS
SA4500-ICE	In Case of Emergency License for SA4500 FIPS
SA4500-ICE-CL	In Case of Emergency Clustering License for SA4500 FIPS
Accessories	
UNIV-MRIU-RAILKIT	Rack mount kit for SA2500 or SA4500 FIPS

MODEL NUMBER	DESCRIPTION
SA6500 FIPS	
Base System	
SA6500FIPS	SA6500 FIPS Base System
User Licenses (Common Access Licensing)	
ACCESSX500-ADD-10U	Add 10 simultaneous users to SA Series or ICX500 Series appliances
ACCESSX500-ADD-25U	Add 25 simultaneous users to SA Series or ICX500 Series appliances
ACCESSX500-ADD-50U	Add 50 simultaneous users to SA Series or ICX500 Series appliances
ACCESSX500-ADD-100U	Add 100 simultaneous users to SA Series or ICX500 Series appliances
ACCESSX500-ADD-250U	Add 250 simultaneous users to SA Series or ICX500 Series appliances
ACCESSX500-ADD-500U	Add 500 simultaneous users to SA Series or ICX500 Series appliances
ACCESSX500-ADD-1000U	Add 1,000 simultaneous users to SA Series or ICX500 Series appliances
ACCESSX500-ADD-2500U	Add 2,500 simultaneous users to SA Series or ICX500 Series appliances
ACCESSX500-ADD-5000U*	Add 5,000 simultaneous users to SA Series or ICX500 Series appliances
ACCESSX500-ADD-7500U*	Add 7,500 simultaneous users to SA Series or ICX500 Series appliances
ACCESSX500-ADD-10KU*	Add 10,000 simultaneous users to SA Series or ICX500 Series appliances
*Multiple SA6500 appliances required	
Feature Licenses	
SA6500-MTG	Secure Meeting for SA6500 FIPS
SA6500-ICE	In Case of Emergency License for SA6500 FIPS
SA6500-ICE-CL	In Case of Emergency Clustering License for SA6500 FIPS

MODEL NUMBER	DESCRIPTION
Accessories	
UNIV-PS-400W-AC	Field upgradeable secondary 400 W power supply for SA6500 FIPS
UNIV-80G-HDD	Field replaceable 80 gigabyte hard disk for SA6500 FIPS
UNIV-MR2U-FAN	Field replaceable fan for SA6500 FIPS
UNIV-MR2U-RAILKIT	Rack mount kit for SA6500 FIPS
UNIV-SFP-FSX	Mini-GBIC transceiver, fiber SX for SA6500 FIPS
UNIV-SFP-FLX	Mini-GBIC transceiver, fiber LX for SA6500 FIPS
UNIV-SFP-COP	Mini-GBIC transceiver - copper for SA6500 FIPS
SA6500-IOC	GBIC I/O card

EES Licenses for SA4500 FIPS and SA6500 FIPS

ACCESS-EES-50U-1YR	Enhanced Endpoint Security subscription, 50 concurrent users, 1-year
ACCESS-EES-100U-1YR	Enhanced Endpoint Security subscription, 100 concurrent users, 1-year
ACCESS-EES-250U-1YR	Enhanced Endpoint Security subscription, 250 concurrent users, 1-year
ACCESS-EES-500U-1YR	Enhanced Endpoint Security subscription, 500 concurrent users, 1-year
ACCESS-EES-1000U-1YR	Enhanced Endpoint Security subscription, 1,000 concurrent users, 1-year
ACCESS-EES-2500U-1YR	Enhanced Endpoint Security subscription, 2,500 concurrent users, 1-year
ACCESS-EES-5000U-1YR	Enhanced Endpoint Security subscription, 5,000 concurrent users, 1-year
ACCESS-EES-7500U-1YR	Enhanced Endpoint Security subscription, 7,500 concurrent users, 1-year
ACCESS-EES-50U-2YR	Enhanced Endpoint Security subscription, 50 concurrent users, 2-year
ACCESS-EES-100U-2YR	Enhanced Endpoint Security subscription, 100 concurrent users, 2-year
ACCESS-EES-250U-2YR	Enhanced Endpoint Security subscription, 250 concurrent users, 2-year
ACCESS-EES-500U-2YR	Enhanced Endpoint Security subscription, 500 concurrent users, 2-year
ACCESS-EES-1000U-2YR	Enhanced Endpoint Security subscription, 1,000 concurrent users, 2-year
ACCESS-EES-2500U-2YR	Enhanced Endpoint Security subscription, 2,500 concurrent users, 2-year
ACCESS-EES-5000U-2YR	Enhanced Endpoint Security subscription, 5,000 concurrent users, 2-year
ACCESS-EES-7500U-2YR	Enhanced Endpoint Security subscription, 7,500 concurrent users, 2-year
ACCESS-EES-50U-3YR	Enhanced Endpoint Security subscription, 50 concurrent users, 3-year
ACCESS-EES-100U-3YR	Enhanced Endpoint Security subscription, 100 concurrent users, 3-year
ACCESS-EES-250U-3YR	Enhanced Endpoint Security subscription, 250 concurrent users, 3-year
ACCESS-EES-500U-3YR	Enhanced Endpoint Security subscription, 500 concurrent users, 3-year
ACCESS-EES-1000U-3YR	Enhanced Endpoint Security subscription, 1,000 concurrent users, 3-year
ACCESS-EES-2500U-3YR	Enhanced Endpoint Security subscription, 2,500 concurrent users, 3-year
ACCESS-EES-5000U-3YR	Enhanced Endpoint Security subscription, 5,000 concurrent users, 3-year
ACCESS-EES-7500U-3YR	Enhanced Endpoint Security subscription, 7,500 concurrent users, 3-year

MODEL NUMBER	DESCRIPTION
Premier RDP Applet Licenses for SA4500 FIPS and SA6500 FIPS	
ACCESS-RDP-50U-1YR	Java RDP Applet 1-year subscription for 50 simultaneous users
ACCESS-RDP-100U-1YR	Java RDP Applet 1-year subscription for 100 simultaneous users
ACCESS-RDP-250U-1YR	Java RDP Applet 1-year subscription for 250 simultaneous users
ACCESS-RDP-500U-1YR	Java RDP Applet 1-year subscription for 500 simultaneous users
ACCESS-RDP-1000U-1YR	Java RDP Applet 1-year subscription for 1,000 simultaneous users
ACCESS-RDP-2000U-1YR	Java RDP Applet 1-year subscription for 2,000 simultaneous users
ACCESS-RDP-2500U-1YR	Java RDP Applet 1-year subscription for 2,500 simultaneous users
ACCESS-RDP-5000U-1YR	Java RDP Applet 1-year subscription for 5,000 simultaneous users
ACCESS-RDP-7500U-1YR	Java RDP Applet 1-year subscription for 7,500 simultaneous users
ACCESS-RDP-10KU-1YR	Java RDP Applet 1-year subscription for 10,000 simultaneous users
ACCESS-RDP-50U-2YR	Java RDP Applet 2-year subscription for 50 simultaneous users
ACCESS-RDP-100U-2YR	Java RDP Applet 2-year subscription for 100 simultaneous users
ACCESS-RDP-250U-2YR	Java RDP Applet 2-year subscription for 250 simultaneous users
ACCESS-RDP-500U-2YR	Java RDP Applet 2-year subscription for 500 simultaneous users
ACCESS-RDP-1000U-2YR	Java RDP Applet 2-year subscription for 1,000 simultaneous users
ACCESS-RDP-2000U-2YR	Java RDP Applet 2-year subscription for 2,000 simultaneous users
ACCESS-RDP-2500U-2YR	Java RDP Applet 2-year subscription for 2,500 simultaneous users
ACCESS-RDP-5000U-2YR	Java RDP Applet 2-year subscription for 5,000 simultaneous users
ACCESS-RDP-7500U-2YR	Java RDP Applet 2-year subscription for 7,500 simultaneous users
ACCESS-RDP-10KU-2YR	Java RDP Applet 2-year subscription for 10,000 simultaneous users
ACCESS-RDP-50U-3YR	Java RDP Applet 3-year subscription for 50 simultaneous users
ACCESS-RDP-100U-3YR	Java RDP Applet 3-year subscription for 100 simultaneous users
ACCESS-RDP-250U-3YR	Java RDP Applet 3-year subscription for 250 simultaneous users
ACCESS-RDP-500U-3YR	Java RDP Applet 3-year subscription for 500 simultaneous users
ACCESS-RDP-1000U-3YR	Java RDP Applet 3-year subscription for 1,000 simultaneous users
ACCESS-RDP-2000U-3YR	Java RDP Applet 3-year subscription for 2,000 simultaneous users
ACCESS-RDP-2500U-3YR	Java RDP Applet 3-year subscription for 2,500 simultaneous users
ACCESS-RDP-5000U-3YR	Java RDP Applet 3-year subscription for 5,000 simultaneous users
ACCESS-RDP-7500U-3YR	Java RDP Applet 3-year subscription for 7,500 simultaneous users
ACCESS-RDP-10KU-3YR	Java RDP Applet 3-year subscription for 10,000 simultaneous users

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.

Copyright 2011 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.