Juniper Networks **Secure Access 4000**

The Juniper Networks Secure Access 4000 (SA 4000) SSL VPN enables mid-to-large-sized organizations to provide cost effective remote and partner extranet access from any standard Web browser. Based on the award-winning Instant Virtual Extranet (IVE) platform, the SA 4000 appliances feature rich access privilege management functionality that can be used to create secure customer/partner extranets with no infrastructure changes, no DMZ deployments, and no software agents. This functionality also allows the enterprise to secure access to the corporate intranet, so that different employee and visitor populations can utilize exactly the resources that they need while adhering to enterprise security policies. Built-in compression for all traffic types speeds performance, and SSL acceleration is available via a software license for more demanding environments.

SA 4000 comes with the streamlined feature set that an enterprise would need to deploy secure remote access, as well as a basic customer/partner extranet or secure intranet. The Advanced license enables additional sophisticated features that meet the needs of more complex deployments with diverse audiences and use cases, as well as Juniper Networks Central Manager.

Value Summary

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

Provision by Purpose

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

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 product line
- Juniper's Endpoint Defense Initiative includes native functionality, client- and server-side APIs and advanced malware protection capabilities for effective enforcement and unified administration of best-of-breed endpoint security

High Availability

- Cluster pair deployment option, for high availability across the LAN and the WAN

Lower Total Cost of Ownership

- Secure remote access with no client software deployments or changes to servers, and virtually no ongoing maintenance
- Secure extranet access with no DMZ buildout, server hardening, resource duplication, or incremental deployments to add applications or users

Streamlined Manageability

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

Access Privilege Management Capabilities

The SA 4000 appliance provides dynamic access privilege management capabilities without infrastructure changes, custom development, or software deployment/maintenance. This facilitates the easy deployment and maintenance of secure remote access, as well as secure extranets and intranets. When a user logs in to the SA 4000, 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.

Features	Benefits
Hybrid role- / resource-based policy model	Administrators can tailor access to dynamically ensure that security policies reflect changing business requirements
Pre-authentication assessment	Network and device attributes, including presence of Host Checker/Cache Cleaner, source IP, browser type and digital certificates, can be examined even before login is allowed and results are used in dynamic policy enforcement decisions
Dynamic authentication policy	Leverages the enterprise's existing investment in directories, PKI, and strong authentication, enabling administrators to establish a dynamic authentication policy for each user session
Dynamic role mapping	Combines network, device and session attributes to determine which of three different types of access is allowed enabling the administrator to provision by purpose for each unique session
Resource authorization	Enables extremely granular access control to the URL, server, or file level to tailor security policies to specific resources
Granular auditing and logging	Fine-grained auditing and logging capabilities in a clear, easy-to-understand format can be configured to the per-user, per-resource, and per-event level. Auditing and logging features can be used for security purposes as well as capacity planning
Custom expressions Advanced software feature set	Enable the dynamic combination of attributes on a "per-session" basis, at the role definition/mapping rules and the resource authorization policy level
Web-based Single Sign-On BASIC Auth & NTLM	Alleviates the need for end users to enter and maintain multiple sets of credentials for Web-based and Microsoft applications
Web-based Single Sign-On Forms-based, Header Variable-based, SAML-based Advance software feature set	In addition to BASIC Auth and NTLM SSO, the advanced feature set provides the ability to pass user name, credentials and other customer defined attributes to the authentication forms of other products and as header variables, to enhance user productivity and provide a customized experience. SAML-based integration for authentication and authorization

Provision by Purpose

The Secure Access 4000 includes 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.

Features	Benefits
Clientless Core Web access	• Access to Web-based applications, including complex JavaScript, XML or Flash-based apps and Java applets that require a socket connection, as well as standards-based e-mail, files and telnet/SSH hosted applications. • Core Web access also enables the delivery of Java applets directly from the Secure Access appliance. • Provides the most easily accessible form of application and resource access, and enables extremely granular security control options
Secure Application Manager (SAM)	• A lightweight Java or Windows-based download 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	• Provides complete network-layer connectivity via an automatically provisioned cross-platform download • Users need only a Web browser. Network Connect transparently selects between two possible transport methods, to automatically deliver the highest performance possible for every network environment.

End-to-End Layered Security

The SA 4000 provides complete end-to-end layered security, including endpoint client, device, data and server layered security controls.
These include:

Features	Benefits
Native Host Checker	Client computers can be checked at the beginning and throughout the session to verify an acceptable security posture requiring or restricting network ports; checking files/process and validating their authenticity with MD5 hash checksums. Performs version checks on security applications, and carries out pre-authentication checks and enforcement. Enables enterprises to write their own host check method to customize the policy checks. Resource access policy for non-compliant endpoints is configurable by the administrator.
Host Checker API	Created in partnership with best-of-breed 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 endpoints
Host Check Server Integration API	Enables enterprises to deliver and update third party security agents from the SA 4000, which reduces public-facing infrastructure, enables consolidated reporting of security events, and enables policy-based remediation of non-compliant clients
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
Hardened security appliance and Web server	Hardened security infrastructure, audited by 3rd party security experts including CyberTrust, effectively protects internal resources and lowers total cost of ownership by minimizing the risk of malicious attacks.
Security services employ kernel-level packet filtering and safe routing	Ensures that unauthenticated connection attempts, such as malformed packets or DOS attacks are filtered out
Custom expressions Advanced software feature set	Enable the dynamic combination of attributes on a "per-session" basis, at the role definition/mapping rules and the resource authorization policy level
Secure Virtual Workspace	Ensures complete data confidentiality with a secure and separate environment for remote sessions that is controlled from copying, printing, or storing data onto an unmanaged PC
Cache Cleaner	All proxy downloads and temp files installed during the session are erased at logout, ensuring that no data is left behind
Data Trap & cache controls	Prevents sensitive meta-data (cookies, headers, form entries, etc) from leaving the network, and allows for rendering of content in a non-cacheable format
Integrated Malware Protection	Enables customers to provision endpoint containment capabilities and secure the endpoint either prior to granting access or during the user session for comprehensive network protection
Coordinated threat control	Enables Juniper's Secure Access SSL VPN and IDP appliances to tie the session identity of the SSL VPN with the threat detection capabilities of IDP to effectively identify, stop, and remediate both network and application-level threats within remote access traffic

Lower Total Cost of Ownership

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

Features	Benefits
Uses SSL, available in all standard Web browsers	Secure remote access with no client software deployment and no changes to existing servers
Based on industry-standard protocols and security methods	The investment in the Secure Access 4000 can be leveraged across many applications and resources over time.
Extensive directory integration & broad interoperability	Existing directories can be leveraged for authentication and authorization. Standard-based interfaces and APIs provide seamless integration with 3rd party products
User self-service features	Increases end user productivity, greatly simplifies administration of large diverse user groups, and lowers support costs, with features that include password management integration and Web Single Sign-On
Multiple Hostname Support Advanced software feature set	Provides the ability to host different virtual extranet Websites from a single SA 4000 appliance, saving the cost of incremental servers, easing management overhead and providing a transparent user experience with differentiated entry URLs
Customizable User Interface Advanced software feature set	Allows the creation of completely customized sign-in pages to give an individualized look for specified roles, streamlining the user experience

High Availability

The SA 4000 includes a variety of capabilities for the availability and redundancy required for mission-critical access in demanding enterprise environments.

Features	Benefits
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 for 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 or across the WAN for superlative scalability with a large number of user licenses, which scales access as the user base grows

Streamlined Management and Administration

The SA 4000 includes a variety of features available from a central management console at the click of a button. These benefits are extended across clustered devices, with the addition of SA Central Manager, part of the Advanced Software features set. Central Manager is a robust product with an intuitive Web-based UI designed to facilitate the task of configuring, updating and monitoring Secure Access appliances whether within a single device, local cluster or across a global cluster deployment.

Features	Benefits
Central Manager Advanced software feature set	Cluster pairs can be seamlessly managed from an integrated central management console, making administration convenient and efficient. The Central Manager allows administrators to track cluster-wide metrics, push configurations and updates, and provide backup and recovery for local and clustered appliances.
User self-service features Password management integration Web Single Sign-On	Increases end user productivity, greatly simplifies administration of large diverse user groups, and lowers support costs
Role-based delegation Advanced software feature set	Granular role-based delegation lessens IT bottlenecks by allowing administrators to delegate control of diverse internal and external user populations to the appropriate parties, associating real-time control with business, geographic, and functional needs.
Easy-to-edit role mapping and resource authorization policies	Administrators can copy and re-use existing policies, simplifying the process of setting up complex multi- variable polices or administration for multiple types of groups/roles
Customizable audit log data Advanced software feature set	Using Secure Access Central Manager, log data can be compiled in standard formats including W3C or WELF, as well as tailored for input into proprietary report packages
SNMP	Enhanced monitoring with standards-based integration to third party management systems

Specifications

Upgrade Options

Hardware
- SSL Acceleration (license enabled)

Software
- Secure Application Manager and Network Connect Upgrade Option (SAMNC)
- Advanced Software Feature Set (includes Central Manager)
- Secure Meeting Upgrade Option
- Instant Virtual System Upgrade Option

Technical Specifications

SA 4000
- Dimensions: 16.7"W x 1.74"H x 15"D
  (42.42cmW x 4.41cmH x 38.10cmD)
- Weight: 13.6lb (6.17kg) typical (unboxed)
- Material: 18 gauge (.048") cold-rolled steel
- Fans: 3, 40mm ball bearing fans, 1 40mm ball bearing fan in power supply
- 19" rack-mountable

Panel Display
- Front Panel Power Button
- Power LED, HD Activity, Temp

Ports

Network
- 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

Console
- One 9-pin serial console port

Power
- AC Power Wattage 260 Watts
- AC Power Voltage 100-240VAC, 50-60Hz, 2.5A Max
- System Battery CR2032 3V lithium coin cell
- Efficiency 65% minimum, at full load
- MTBF 70,000 hours

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

Safety and Emissions Certification
- Safety: EN60950-1:2001 + A11, UL60950-1:2003, CSA C22.2 No. 60950-1, IEC 60950-1:2001
- Emissions: FCC Class A, VCCI Class A, CE class A

Warranty
- 90 days – can be extended with support contract

Other
- Common Criteria Certified
- FIPS Appliances Available

Ordering Information

Secure Access 4000 Base System

SA4000	Secure Access 4000 Base System

Secure Access 4000 User Licenses

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

Secure Access 4000 Feature Licenses

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

Secure Access 4000 Clustering Licenses

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

Accessories

SA-ACC-RCKMT-KIT-1U	Spare Secure Access Rack Mount Kit - 1U
SA-ACC-PWR-AC-USA	Spare Secure Access AC Power Cord USA
SA-ACC-PWR-AC-UK	Spare Secure Access AC Power Cord UK
SA-ACC-PWR-AC-EUR	Spare Secure Access AC Power Cord EUR
SA-ACC-PWR-AC-JPN	Spare Secure Access AC Power Cord JPN