

Juniper Networks Secure Access 4000 FIPS



Proven Secure Access That Complies with Stringent U. S., Canadian and UK Security Standards

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 meet the rigors of government communication standards and have been certified to that effect. While these strictures are actually required for some government agencies, they also provide useful guidelines to private sector businesses that require stringent security. Juniper Networks uniquely delivers on these needs with proven solutions that provide the most flexible secure access available among U. S. government-certified solutions.

FIPS-Compliant Security with the Ease of the Instant Virtual Extranet

Juniper Networks is the market leader in SSL based remote access that is easy to deploy and easy to maintain. Built on the Instant Virtual Extranet (IVE) platform, all Juniper Networks Secure Access SSL VPN appliances have met or exceeded the stringent security standards of independent Internet security auditing agencies. Juniper Networks extends this leadership with a FIPS-compliant offering, combining all of the features of the award-winning IVE platform with a FIPS-certified hardware security module. Like all Secure Access products, the SA4000 FIPS appliance is a hardened security gateway that uses the standards based Secure Sockets Layer (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 or firewall traversal issues to contend with, and virtually no ongoing maintenance. SSL itself 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 compared to traditional VPNs or custom extranets, and a highly scalable implementation.

Value Summary

FIPS Security

- Stringent security with a FIPS certified hardware security module

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

FIPS Security

The FIPS appliances build on the IVE secure platform, incorporating a FIPS certified Hardware Security Module (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 Secure Access FIPS appliances also have a tamper evident label that deters physical security breaches and provides visual indication of appliance integrity.

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

Features	Benefits
<ul style="list-style-type: none"> • Complies with the latest US Government Best Practices • FIPS140-2 Level 3 Certified Hardware Security Module • 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 	<p>Advanced protection to provide the most stringent security</p>

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	<ul style="list-style-type: none"> • 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)	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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

Software

- Secure Application Manager and Network Connect Upgrade Option (SAMNC)
- Advanced Software Feature Set (includes Central Manager)
- Secure Meeting 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: 15.9lb (7.21kg) 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
- FIPS Status LED
- HSM Status LED

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 65,000 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 95 % 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

Ordering Information

Secure Access 4000 FIPS Base System

SA4000FIPS	Secure Access 4000 FIPS 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
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



CORPORATE HEADQUARTERS
AND SALES HEADQUARTERS
FOR NORTH AND SOUTH AMERICA
Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
Phone: 888-JUNIPER (888-586-4737)
or 408-745-2000
Fax: 408-745-2100
www.juniper.net

EAST COAST OFFICE
Juniper Networks, Inc.
10 Technology Park Drive
Westford, MA 01886-3146 USA
Phone: 978-589-5800
Fax: 978-589-0800

ASIA PACIFIC REGIONAL
SALES HEADQUARTERS
Juniper Networks (Hong Kong) Ltd.
Suite 2507-11, 25/F
ICBC Tower
Citibank Plaza, 3 Garden Road
Central, Hong Kong
Phone: 852-2332-3636
Fax: 852-2574-7803

EUROPE, MIDDLE EAST, AFRICA
REGIONAL SALES HEADQUARTERS
Juniper Networks (UK) Limited
Building 1
Aviator Park
Station Road
Aldrestone
Surrey, KT15 2PG, U.K.
Phone: 44-(0)-1372-385500
Fax: 44-(0)-1372-385501

Copyright 2006, Juniper Networks, Inc. All rights reserved.

Juniper Networks and the Juniper Networks logo are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered trademarks, or registered service marks in this document are the property of Juniper Networks or their respective owners. All specifications are subject to change without notice. Juniper Networks assumes no responsibility for any inaccuracies in this document or for any obligation to update information in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.