

Juniper Networks Secure Access 700



The Juniper Networks Secure Access 700 (SA 700) SSL VPN appliance provides small to medium enterprises a secure, cost-effective way to deploy remote access to the corporate network. Because the SA 700 uses Secure Sockets Layer (SSL) to provide encrypted transport, it enables instant remote access from just a Web browser. This clientless architecture eliminates the high cost of installing, configuring, and maintaining client software on every device, significantly reducing the total cost of ownership versus traditional VPN solutions. SSL delivery also eliminates the Network Address Translation (NAT) and firewall traversal issues encountered with traditional remote access products, allowing your remote users reliable and ubiquitous access from external networks such as home or hotels. The SA 700 comes standard with Juniper Networks Network Connect access method, which creates a secure network-layer connection via a lightweight, cross-platform dynamic download. The SA 700 can also be upgraded to include Juniper's Core Clientless access method, which enables connections from any PC anywhere to Web-enabled applications, files, XML and Flash content. Built on Juniper's market-leading Instant Virtual Extranet (IVE) platform, the Secure Access 700 series delivers enterprise-strength AAA (authentication, authorization, auditing), comprehensive endpoint defense, and a core security architecture that has been audited in depth by CyberTrust and certified by ICSA labs.

Value Summary

Lower Total Cost of Ownership

- Dependable technology tailored to the needs of small to mid-sized enterprises by the SSL VPN market leader – Juniper Networks
- Plug-n-play appliance that installs in minutes with minimal IT knowledge required
- No client software deployment or maintenance – users only need an internet connection for access
- Simple end user and administrator interfaces facilitate quick and easy use
- Improved productivity for remote employees
- No network interoperability issues

End-to-End Security

- Complete, secure access to LAN resources, ensuring that the endpoint device, data in transit, and internal resources are secure
- Seamless integration with broad range of authentication methods and protocols
- Juniper's Endpoint Defense Initiative includes native functionality and client- and server-side APIs for effective enforcement and unified administration of best-of-breed endpoint security

Lower Total Cost of Ownership

The Secure Access 700 deploys quickly and easily and does not require the costly deployment and maintenance of individual client software on each device. The SA 700 delivers an appliance tailored to the specific needs of small to mid-sized companies, in an affordable plug-n-play form factor.

Features	Benefits
Uses SSL, available in all standard Web browsers	Enables secure remote access from any browser
No end-user client to install	<ul style="list-style-type: none"> • Requires no changes to existing network infrastructure • Eliminates the cost and complexity associated with maintaining installed clients on user PCs • Supports multiple operating systems, including Windows, Linux, Mac, PocketPC and more • Add new users or access to new applications with just a few clicks
Leverages existing security infrastructure	<ul style="list-style-type: none"> • Integrates with existing user directories • Fully compatible with a broad range of authentication methods and protocols
Interoperation with external networks – eliminating issues with network address translation (NAT) or firewall traversal	<ul style="list-style-type: none"> • Improves user experience by simplifying access to internal resources from external networks • Reduces costly support calls
Desktop or 1U rack-mountable form factor	Runs quietly on desktop if no server rack available
Individual models provide support for 10 or 25 concurrent users	Offers customers the flexibility to purchase according to their capacity requirements and budgetary limitations

End-to-End Layered Security

The SA 700 series provides complete end-to-end layered security, ensuring that the endpoint device, data in transit, and internal resources are secure. The SA 700 integrates seamlessly with a broad range of authentication methods and protocols and its hardened architecture effectively protects internal resources. Security features 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 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 700, which reduces public-facing infrastructure, enables consolidated reporting of security events, and enables policy-based remediation of non-compliant clients
Hardened security appliance and Web server	Purpose-built hardware appliance and hardened security infrastructure, with no general purpose services, system-level user accounts, or interactive shell
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
Cache Cleaner	All proxy downloads and temp files installed during the session are erased at logout, ensuring that no data is left behind
Support for strong authentication methods and protocols including RADIUS, LDAP PKI, Active Directory, RSA/Secure ID	Enables enterprise-strength authentication via optional integration with directories, PKI, and leading multi-factor authentication systems. Allows administrators to establish dynamic authentication policies for each user session, based on user/device/network attributes and specific login conditions, including an optional pre-authentication assessment to examine the client's security state before the login page is presented. Also includes a secure internal user database for enterprises that have not deployed 3rd party authentication.
Auditing and logging	Full auditing and logging capabilities in a clear, easy-to-understand format, simplifying configuration, assessment and troubleshooting

Ease of Use

The SA 700 features a user-friendly Web-based interface and streamlined administration making it easy to use and administer.

Features	Benefits
Streamlined administration process designed specifically for small/medium enterprises	Instant deployment and activation requires minimal IT knowledge
Dynamically provisioned user connectivity	At login, end users are immediately provisioned full connectivity as if running on the LAN, while important layered security functions run transparently. Users provisioned using the Core Clientless access method upgrade are restricted to administrator configurable Web-based applications
Simple, Web-based interfaces	Both the end user and administrator interfaces are simple and Web-based, facilitating quick and easy use

Provision by Purpose

The Secure Access 700 includes two 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
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
Clientless Core Web access (Available as an upgrade)	<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

Specifications

Upgrade Options

- Software
- Core Clientless Access Upgrade Option

Technical Specifications

SA 700

- Dimensions: 17.25"W x 1.74"H x 9"D
(43.80cmW x 4.41cmH x 22.86cmD)
- Weight: 10lb (4.53 kg) typical (unboxed)
- Material: 18 gauge (.048") aluminum
- Fans: 1 ball-bearing inlet fan, plus 1 CPU blower

Panel Display

- Front Panel Power Switch
- Power LED
- Access LED (drive access)

Ports

Network

- Two RJ-45 Ethernet
- 10/100 full or half-duplex (auto-negotiation)
- IEEE 802.3 compliant

Console

- One 9-pin serial console port

Power

- Input Voltage and Current 90-264 VAC Full Range
- 4A (RMS) at 90 VAC
- 2A (RMS) at 264 VAC
- Input Frequency 47-63Hz
- Efficiency 65% min, at full load
- Output power 220w
- Power Supply MTBF 100,000 hours at 25°C

Environmental

- Temperature Range Operating: 5C to 30C (41F to 86F)
- Operating (short-term): 0C to 50C (32F to 122F)
- Non-Operating: -30C to 60C (-22F to 140F)
- Relative Humidity (Operating) 20% to 80% noncondensing
- Relative Humidity (Non-Operating) 5% to 95% noncondensing
- Altitude: to 10,000 ft (3,000m)
- Shock Operating: 2G at 11ms
- Non-Operating: 30G at 11ms

Safety and Emissions Certification

- Safety: UL (UL 60950-1 First Edition: 2003)
CUL (CAN/CSA-C22.2 No. 60950-1-03 First Edition)
TUV GS (EN 60950-1:2002)
AS/NZS CISPR 22: 2002, Class B
- Emissions: FCC Class B, VCCI Class B, CE class B



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, Asia Pacific Finance 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
Juniper House
Guildford Road
Leatherhead
Surrey, KT22 9JH, U. K.
Phone: 44(0)1372-385500
Fax: 44(0)1372-385501

Copyright 2005, 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.

100124-001 July 2005

Authorized Partner:



InfoGuard AG, Feldstrasse 1, CH-6300 Zug
Telefon +41 41 749 19 00, Telefax +41 41 749 19 10
info@infoguard.com, www.infoguard.com