



# Juniper Networks Secure Access 700 Appliance

*The Juniper Networks Secure Access 700 (SA 700) SSL VPN appliance enables small to medium sized enterprises to deploy remote access to the corporate network in a secure and cost-effective way. 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 (TCO) versus traditional VPN solutions. SSL delivery also eliminates the Network Address Translation (NAT) and firewall traversal issues encountered with traditional remote access products, allowing remote & mobile users reliable and ubiquitous access from external networks such as home or hotels.*

## Product Description

The Juniper Networks Secure Access 700 comes standard with 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 Core Clientless access method, which enables connections from any device at any location to Web-enabled applications, including those with XML and Flash content, files, standards-based email, and telnet/SSH sessions. The Secure Access 700 appliance delivers enterprise-strength AAA (authentication, authorization, and accounting) and comprehensive endpoint defense.

## Architecture and Key Components

### Lower TCO

- 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.

## Features and Benefits

The Secure Access 700 deploys quickly and easily, and it 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.

Table 1. SA 700 Lower Cost of Ownership

Feature	Feature Description	Benefit
Uses SSL, available in all standard Web browsers	Enables secure remote access from any browser	Users only need an Internet connection for access
No end user client to install	<ul style="list-style-type: none"> <li>Requires no changes to existing network infrastructure</li> <li>Supports multiple operating systems, including Windows, Linux, Mac, PocketPC and more</li> </ul>	<ul style="list-style-type: none"> <li>Eliminates the cost and complexity associated with maintaining installed clients on user devices</li> <li>Enables the addition of new users or access to new applications with just a few clicks</li> </ul>
Leverages existing security infrastructure	<ul style="list-style-type: none"> <li>Integrates with existing user directories</li> <li>Fully compatible with a broad range of authentication methods and protocols</li> </ul>	Simplifies any network administration
Interoperation with external networks—eliminating issues with (NAT) or firewall traversal	<ul style="list-style-type: none"> <li>Improves user experience by simplifying access to internal resources from external networks</li> <li>Reduces costly support calls</li> </ul>	Eliminates network interoperability issues
Desktop or 1U rack-mountable form factor	Runs quietly on desktop if no server rack available	Saves valuable rack space in the data closet
Individual models provide support for 10, 15, or 25 concurrent users	Offers customers the flexibility to purchase according to their capacity requirements and budgetary limitations	IT investments can be made according to budget and need

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.

Table 2. SA 700 End-to-End Layered Security

Feature	Feature Description	Benefit
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/processes, and validating their authenticity with Message Digest 5 (MD5) hash checksums. Performs version checks on security applications, and carries out pre-authentication checks and enforcement.	<ul style="list-style-type: none"> <li>Enables enterprises to write their own host checker method to customize the policy checks.</li> <li>Resource access policy for non-compliant endpoints is configurable by administrator.</li> </ul>
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.	Uses current security policies with remote users and devices; easier management.
Host Checker Server Integration API	Enables enterprises to deliver and update third-party security agents from the SA 700.	<ul style="list-style-type: none"> <li>Reduces public-facing infrastructure.</li> <li>Enables consolidated reporting of security events.</li> <li>Enables policy-based remediation of non-compliant clients.</li> </ul>
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.	Not designed to run any additional services and is less susceptible to attacks; no backdoors to exploit.
Security services employ kernel-level packet filtering and safe routing	Ensures that unauthenticated connection attempts, such as malformed packets or denial of service (DoS) attacks, are filtered out.	Effective protection against threats and attacks.
Cache Cleaner	All proxy downloads and temp files installed during the session are erased at logout, ensuring that no data is left behind.	Ensures that no potentially sensitive session data is left behind on the endpoint machine.
Support for strong authentication methods and protocols including RADIUS, Lightweight Directory Access Protocol (LDAP), public key infrastructure (PKI), Active Directory, RSA/Secure ID	Enables enterprise-strength authentication via optional integration with directories (PKI) and leading multi-factor authentication systems. Also includes a secure internal user database for enterprises that have not deployed third-party authentication.	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.
Auditing and logging	Full auditing and logging capabilities in a clear, easy-to-understand format.	Simplifies configuration, assessment and troubleshooting.
Malware protection	Enables customers to provision endpoint containment capabilities and secure the endpoint either prior to granting access or during the user session.	Provides comprehensive network protection.

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

Table 3. SA 700 Ease of Use

Feature	Feature Description	Benefit
<b>Streamlined administration process designed specifically for small/medium enterprises</b>	Instant deployment and activation requires minimal IT knowledge.	Increased productivity for IT resources.
<b>Dynamically provisioned user connectivity</b>	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.	Flexibility of allowing users access to different types of resources.
<b>Simple, Web-based interfaces</b>	Both the end user and administrator interfaces are simple and Web-based, facilitating quick and easy use.	Enables end user and administrator productivity.

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.

Table 4. SA 700 Provision by Purpose

Feature	Feature Description	Benefit
<b>Network Connect</b>	Provides complete network-layer connectivity via an automatically provisioned cross-platform download.	<ul style="list-style-type: none"> <li>• Users only need a Web browser for access.</li> <li>• Network Connect transparently selects between two possible transport methods to automatically deliver the highest performance possible for every network environment.</li> </ul>
<b>Clientless Core Web access (Available as an upgrade)</b>	<ul style="list-style-type: none"> <li>• 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 email, files and telnet/SSH hosted applications.</li> <li>• Core Web access also enables the delivery of Java applets directly from the Secure Access appliance.</li> </ul>	<ul style="list-style-type: none"> <li>• Provides the most easily accessible form of application and resource access.</li> <li>• Enables extremely granular security control options.</li> </ul>

## Product Options

Core Clientless Access Upgrade

### Specifications

#### SA 700

- Dimensions (W x H x D): 17.25 x 1.74 x 9 in (43.80 x 4.41 x 22.86 cm)
- Weight: 10 lb (4.53 kg) typical (unboxed)
- Material: 18 gauge (.048 in) 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
- 4 A (RMS) at 90 VAC
- 2 A (RMS) at 264 VAC
- Input Frequency 47-63 Hz
- Efficiency 65% min, at full load
- Output power 220 W
- Power Supply mean time between failures (MTBF) 100,000 hours at 25° C

##### Environmental

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

**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

**Ordering Information**

Model Number	Description
<b>Secure Access 700 Base System</b>	
SA700	Secure Access 700 Base System
<b>Secure Access 700 User Licenses</b>	
SA700-ADD-10U	Add 10 simultaneous users to SA 700
SA700-ADD-15U	Add 15 simultaneous users to SA 700
SA700-ADD-25U	Add 25 simultaneous users to SA 700
<b>Secure Access 700 Feature Licenses</b>	
SA700-CORE	Core Clientless Web Access for SA 700

**About Juniper Networks**

Juniper Networks, Inc. is the leader in high-performance networking. Juniper offers a high-performance network infrastructure that creates a responsive and trusted environment for accelerating the deployment of services and applications over a single network. This fuels high-performance businesses. Additional information can be found at [www.juniper.net](http://www.juniper.net).



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](http://www.juniper.net)

EUROPE, MIDDLE EAST, AFRICA  
REGIONAL SALES HEADQUARTERS  
Juniper Networks (UK) Limited  
Building 1  
Aviator Park  
Station Road  
Addlestone  
Surrey, KT15 2PG, U.K.  
Phone: 44.(0).1372.385500  
Fax: 44.(0).1372.385501

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.  
26/F, Cityplaza One  
1111 King's Road  
Taikoo Shing, Hong Kong  
Phone: 852.2332.3636  
Fax: 852.2574.7803

Copyright 2008 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. JUNOS and JUNOSe are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, 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.

To purchase Juniper Networks solutions, please contact your Juniper Networks sales representative at 1-866-298-6428 or authorized reseller.