JUNIPER SECURE CONNECT DATASHEET

Product Overview

Juniper Secure Connect is a highly flexible SSL VPN application that gives remote workers secure access to corporate and cloud resources, providing reliable connectivity and consistent security to any device, anywhere. Juniper Secure Connect is available for desktop and mobile devices including Windows, Mac OS, Android, and iOS. When combined with the SRX Series Firewalls, it helps organizations quickly achieve optimal performance and connectivity from client to cloud, reducing risk by extending visibility and enforcement to users and devices, wherever they are.

Product Description

Organizations are growing increasingly distributed, driven largely by work-from-home initiatives, branch expansion, and growth of temporary pop-up sites. Securing this distributed traffic requires deep network visibility and the ability to enforce policy at every connection point—capabilities that separate secure SD-WANs from traditional network access methods.

Juniper® Secure Connect allows organizations to provide secure end-user access across their WAN fabrics. Working with Juniper Networks SRX Series Firewalls as the head-end SSL VPN and IPsec termination point, deployed on campus, in a data center, or in the cloud, Juniper Secure Connect enables secure access to vital resources from user devices running Windows, MacOS, iOS, and Android. To simplify deployment of Juniper Secure Connect, the client application ensures that the most current policy is being used, with no end-user or admin interaction required to reduce deployment time and ongoing troubleshooting.

Architecture and Key Components

Offered as an add-on license for SRX Series Firewalls, Juniper Secure Connect provides secure access for users who need remote access to protected resources across the Internet from wherever they happen to be. SRX Series Firewalls are available as physical appliances as well as in virtualized and containerized form factors, providing the connectivity and network security required for organizations to build a secure SD-WAN fabric.

The Juniper Secure Connect application offers additional features that increase security and usability. These features include multifactor and biometric authentication, automatic policy validation before a connection is established, and Windows pre-domain logon to ensure that the Windows devices are validated and update the latest Active Directory Group Policy during logon.

Security policies can be applied to devices operating outside the corporate network via Juniper Secure Connect, treating the traffic as if it were untrusted. Juniper Networks AppSecure, intrusion prevention system (IPS), content security, and advanced threat detection policies configured on SRX Series firewalls are extended to these remote devices, ensuring that consistent security is applied to all points of presence, wherever they are located, and providing the appropriate level of secure access for every type of connection.

This consistent security policy application allows users to be part of a larger secure SD-WAN fabric that empowers organizations to deliver reliable connectivity and threat protection to and from branch offices, temporary pop-up sites, and home offices, as well as employees operating remotely from within other networks such as those at hotels or conferences. Juniper secure SD-WANs allow traffic management and security policies to be applied on a per-data flow basis.

Data flows can be identified by application, user, IP address, and URL, allowing IT teams to prioritize or more deeply inspect some of those data flows. Individual data flows can also be routed independently where multiple WAN fabric access options exist. This flexibility allows Juniper secure SD-WANs to reduce both capital costs and administrative overhead compared to traditional WAN access, while providing the security needed to handle both known and unknown threats. With Juniper Secure Connect, policy can be set to require all traffic to be routed through the VPN connection or configured to support split tunneling, ensuring that traffic can take the best and most secure path.

Features and Benefits

Feature	Description	Benefit
Available for desktop and mobile devices	Juniper Secure Connect is available for Windows, MacOS, iOS, and Android operating systems.	Provides flexible and secure access for managed and unmanaged devices.
Zero-touch configuration	Juniper Secure Connect uses a secure and automatic validation of the most current policy, making sure users always get the correct security policy enforced.	Offers an always up-to-date security policy, ensuring users stay secure and get access to the correct resources at any time.
Multifactor and biometric authentication	To increase security, Juniper Secure Connect supports multifactor authentication from industry-leading multifactor authentication (MFA) solutions. It also supports integrated biometric authentication on devices with the hardware support.	Improves corporate security by leveraging a second form of authentication for remote users.
Comprehensive security and visibility	User access coming via Juniper Secure Connect must be subject to IPS, Juniper Advanced Threat Prevention, and advanced security to identify and block unknown and known threats that originate from non-corporate networks.	Reduces risk and provides the necessary visibility to ensure that remote access users are not introducing known or unknown threats.

Specifications

Features	Windows	MacOS	iOS	Android
OS versions	10.x or higher	10.13, 10.14, 10.15	9.3 or higher	4.4 or higher
Next-generation cryptography	Yes			
Client SSL VPN	Yes			
Dead peer detection (DPD)	Yes			
Split tunneling	Yes			
Multifactor authentication (MFA)	Yes			
Biometric authentication	Yes			
Zero-touch app configuration	Yes			
Windows pre-domain logon	Yes	No	No	No
Juniper Secure Connect license and support duration	1 or 3 years			

Table 1. SRX Series Concurrent Users Supported

SRX Series Firewall Model	Concurrent Remote Access/SSL VPN Users Supported
SRX300 Firewall	25
SRX320 Firewall	50
SRX340 Firewall	150
SRX345 Firewall	250
SRX380 Firewall	500
SRX550M Firewall	500
SRX1500 Firewall	2000
SRX4100 Firewall	7500
SRX4200 Firewall	7500
SRX4600 Firewall	7500
SRX5400 Firewall	25,000
SRX5600 Firewall	40,000
SRX5800 Firewall	50,000
vSRX Virtual Firewall	500

Ordering Information

To order Juniper Secure Connect, and to access software licensing information, please visit the How to Buy page on www.juniper.net. The Juniper Secure Connect licenses below are stackable and license usage is based on current users connected to the head-end SRX Series firewall.

About Juniper Networks

At Juniper Networks, we are dedicated to dramatically simplifying network operations and driving superior experiences for end users. Our solutions deliver industry-leading insight, automation, security and AI to drive real business results. We believe that powering connections will bring us closer together while empowering us all to solve the world's greatest challenges of well-being, sustainability and equality.

Corporate and Sales Headquarters

Juniper Networks, Inc.

1133 Innovation Way

Sunnyvale, CA 94089 USA

Phone: 888.JUNIPER (888.586.4737)

or +1.408.745.2000

www.juniper.net

APAC and EMEA Headquarters

Juniper Networks International B.V.

Boeing Avenue 240 1119 PZ Schiphol-Rijk

Amsterdam, The Netherlands

Phone: +31.207.125.700