JUNIPER SECURE CONNECT DATASHEET

Product overview

Juniper Secure Connect is a highly flexible SSL VPN and IPsec 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, Apple macOS, iOS, iPadOS, and Android. 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, primarily driven by remote work and branch expansion. Securing this distributed traffic requires deep network visibility and the ability to enforce policy at every connection point.

Juniper® Secure Connect allows organizations to provide secure end user access by leveraging IP connectivity. 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 the cloud, Juniper Secure Connect enables secure access to vital resources from user devices running Windows, Apple macOS, iOS, iPadOS, and Android. Deploying Secure Connect is simple: The client application must ensure that the most current policy is used at every connection. No end user or admin interaction is 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 leverages IP connectivity to provide secure access for users from anywhere. Juniper Secure Connect works with SRX Series Firewalls in physical, virtual, and as-a-service form factors, providing connectivity and network security to support users, devices, and data wherever they are.

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

Security policies are applied to devices via Juniper Secure Connect. These policies might treat this traffic as if it were untrusted. Secure Connect leverages Juniper Networks' AppSecure, intrusion prevention system (IPS), content security, and advanced threat prevention to extend security to remote devices. This ensures consistent security across the entire network and provides the appropriate level of secure access.

Juniper Secure Connect leverages consistent security policies that allow organizations to deliver effective threat protection to and from branch offices and home offices and employees working remotely from within other networks, enabling organizations to ensure secure architectures and experiences.

Data flows can be identified by the application, user, IP address, and URL, allowing IT teams to prioritize or more deeply inspect some of those data flows. With Juniper Secure Connect, the policy can 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	Available for Windows, Apple macOS, iOS, iPadOS, and Android operating systems.	Provides flexible and secure access for managed and unmanaged devices.
Zero-touch configuration	Uses secure and automatic validation of the most current policy, ensuring 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	Supports external multifactor authentication from industry-leading multifactor authentication (MFA) solutions to increase security. It also supports integrated biometric authentication on devices with 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 remote access users are not introducing known or unknown threats.

Juniper Security Director Cloud

Security Director Cloud is Juniper's simple and seamless management experience delivered in a single UI to connect customers' current deployments with their future architectural rollouts. Management is at the center of the Juniper Connected Security strategy and helps organizations secure every point of connection on their network to safeguard users, data, and infrastructure.

Organizations can secure their architecture with consistent security policies across any environment—on premises, cloud-based, cloud-delivered, and hybrid—and expand Zero Trust to all parts of the network, from the edge to the data center to the applications and microservices. With Security Director Cloud, organizations have unbroken visibility, policy configuration, administration, and collective threat intelligence all in one place.

Juniper meets our customers where they are on their architectural journey, helps them leverage their existing investments, and empowers them to transition to their preferred architecture at a pace that is best for business by automating their transition with Security Director Cloud.

Juniper Secure Edge

Juniper Secure Edge secures workforces anywhere with the fast, reliable, and secure access they need. It delivers full-stack SSE capabilities, including FWaaS, SWG, and CASB with DLP, ZTNA, and advanced threat protection to protect access to web, SaaS, and on-premises applications and provide users with security that follows them wherever they go. Juniper meets customers where they are and takes them where they want to go by leveraging what they have and extending their Zero Trust initiatives to a cloud-delivered architecture without breaking the bank or their ops team.

Juniper Secure Edge, managed by Security Director Cloud, uses a single policy framework that enables security policies to be created once to follow users, devices, and data wherever they go. Customers don't have to start from scratch when adopting cloud-delivered security. With our three-click wizard, customers can easily leverage existing campus edge policies and translate them into an SSE policy. Because it uses a single policy framework regardless of the deployment model, Secure Edge applies existing security policies from traditional deployments to its cloud-delivered model in just a few clicks, reducing misconfigurations and risk.

Whether securing remote users, campus and branch locations, private cloud, public cloud, or hybrid cloud data centers, Juniper provides unified management and unbroken visibility across all architectures. This makes it easy for ops teams to effectively bridge their current investments with future architectural goals, including SASE. Customers can manage security anywhere and everywhere, on-premises, in the cloud, and from the cloud, with security policies that follow users, devices, and data wherever they go, all from a single UI.

Users have fast, reliable, and secure access to the data and resources they need, ensuring great user experiences. IT security teams gain seamless visibility across the entire network while leveraging their existing investments, helping them transition to a cloud-delivered architecture at their own pace.

Juniper Secure Edge provides consistent security policies that follow the user, device, and data without having to copy over or recreate rule sets. It's easy to deploy cloud-delivered application control, intrusion prevention, content and web filtering, and effective threat prevention without breaking visibility or security enforcement.

Multiple third-party tests have consistently validated Juniper as the most effective security technology on the market for the past five years, with over 99% security efficacy across all use cases.

Specifications

Features	Windows	MacOS	iOS/iPadOS	Android
Next-generation cryptography	Yes	Yes	Yes	Yes
Client-based SSL VPN	Yes	Yes	Yes	Yes
Dead peer detection (DPD)	Yes	Yes	Yes	Yes
Split tunneling	Yes	Yes	Yes	Yes
Multifactor authentication (MFA)	Yes	Yes	Yes	Yes
Biometric authentication	Yes	Yes	Yes	Yes
Zero-touch app configuration	Yes	Yes	Yes	Yes
Pre-logon compliance checks	Yes	Yes	Yes	Yes
Juniper Secure Connect license and support duration	1, 3, or 5 year			

Ordering information

To get started with Juniper Secure Connect and to access software licensing information, use the following links from Juniper's support site:

- Windows
- macOS
- iOS/iPadOS
- Android

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

About Juniper Networks

Juniper Networks believes that connectivity is not the same as experiencing a great connection. Juniper's AI-Native Networking Platform is built from the ground up to leverage AI to deliver exceptional, highly secure, and sustainable user experiences from the edge to the data center and cloud. Additional information can be found at juniper.net or connect with Juniper on X (formerly Twitter), LinkedIn, and Facebook.

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

Juniper Networks | Driven by Experience™