Secure, AI-Driven SD-WAN

Session Smart Router Security Capabilities at-a-Glance

Security has never been more critical for enterprises networking teams. Juniper Networks® Session Smart™ Routers (SSRs), the routing core of Juniper AI-Driven SD-WAN, are designed from the ground up with a full set of security features throughout the networking fabric to safeguards users and data. A multitude of features are inherently included in the SSR, and more features can be added with the Advanced Security Pack.

Inherent Security Features in the Session Smart Router (SSR)

- ✓ Centralized management
- ✓ Full encryption
- ✓ Zero Trust Model
- ✓ Route directionality, Policy enforcement
- ✓ Layer 3/Layer 4 Firewall
- ✓ FIPS 140-2 & JITC certified
- ✓ Fine-grained segmentation

SSR SECURITY
SSR
+
ADVANCED SECURITY PACK

SSR Advanced Security Pack

IPS/IDS

URL Web filtering

Session Smart Router Baseline Security and Advanced Security Pack

Inherent Security Features of the Session Smart Router

Feature	Benefit	Feature	Benefit
Centralized Management	Enables automated, simplified, and scalable security policies	Policy Enforcement	Verifies and enforces policies at every hop
Full Encryption	Leverages adaptive encryption to eliminate overhead	Layer 3/4 Firewall	Inspects and filters traffic based on IP addresses, ports, and protocols
Zero Trust Model	Drops sessions that do not have explicit allow policies	FIPS 140-2 and JITC certified	Adheres to government security standards for firewall functionality
Route Directionality	Unifies access control and security policies during routing	Fine-Grained Segmentation	Protects users, groups, and applications with per-service access policies

Advanced Security Pack Features

Feature	Benefit
Intrusion prevention system and intrusion detection system (IPS/IDS)	Protects against malicious attacks with IPS and IDS
URL Web filtering	Prevents access to and from specific sites to meet special business needs

Secure Edge Connectors

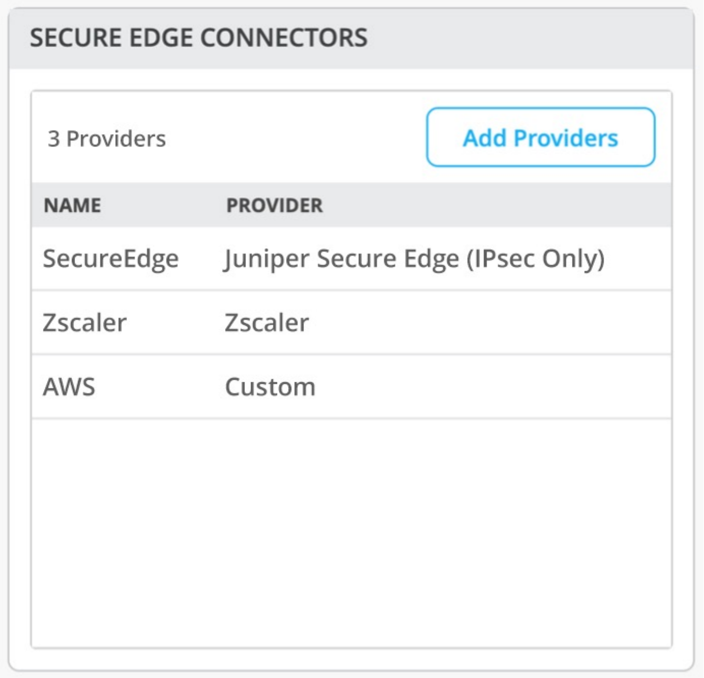
For a complete Secure Access Service Edge (SASE) solution, Juniper Secure Edge connectors in the Juniper Mist™ Cloud enable seamless integrations from Juniper AI-Driven SD-WAN to any Secure Services Edge (SSE).

Secure Edge connectors make it easy to offload traffic from an SSR to an SSE. Administrators simply input corresponding information (such as pre-shared key and hostname/IP address) in the Juniper Mist Cloud and in the SSE to create Secure Edge connections.

Two connector types are pre-built in the Juniper Mist Cloud:

- Juniper Secure Edge
- Zscaler

Additionally, if you have an SSE that is not Juniper Secure Edge or Zscaler, you can still use a custom, easy-to-build Secure Edge connector.



SECURE EDGE CONNECTORS

3 Providers

NAME	PROVIDER
SecureEdge	Juniper Secure Edge (IPsec Only)
Zscaler	Zscaler
AWS	Custom

Learn more about Juniper's Secure SD-WAN solution.

- Get the White Paper: AI-Driven SD-WAN Secures Today's Cloud-Era Networks
- Read the Solution Brief: AI-driven SD-WAN: Building Networks with Security at Their Core

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
Fax: +1.408.745.2100
www.juniper.net

APAC and EMEA Headquarters
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
Phone: +31.0.207.125.700
Fax: +31.0.207.125.701

Driven by Experience™