ENABLING SASE WITH JUNIPER AI-DRIVEN SD-WAN

Experience-First Security for Distributed Sites and Cloud Service Edges

White Paper

©2022, Juniper Networks, Inc.

TABLE OF CONTENTS

Enterprise Networking Trends

- *An increase in distributed workplaces and remote workers needing secure and reliable access to public and private cloud services*

Industry Direction

- *Secure Access Service Edge (SASE) functionality including SD-WAN for scalable, secure connectivity and Secure Services Edge (SSE) features for cloud-based security*

Benefits

- *Juniper AI-driven SD-WAN provides the ideal foundation for an enterprise-wide SASE architecture. When combined with cloud-based security functionality such as the Juniper Secure Edge, enterprises can secure any number of sites, users, and applications, while enjoying 30% to 50% bandwidth savings and unencumbered multicloud access.*[1]

[1] ASG Research, Tunnel-based vs. Tunnel Free SD-WAN, Ray Mota, PhD, 2020

©2022, Juniper Networks, Inc.

EXECUTIVE SUMMARY

The modern distributed workplace—including enterprises with thousands of branches and remote workers—requires updated approaches to cloud, networking, and security infrastructure. Cloud migration has opened the door to a huge increase in sophisticated applications, requiring networks that can carry traffic to an increasingly remote workforce. In turn, this creates a unique set of new requirements for security, including special capabilities to handle unpredictable locations of users, applications, and traffic flows.

A highly secure and efficient SD-WAN provides the ideal basis for enterprise-wide Secure Access Service Edge (SASE). Recognizing that security must be fully integrated into the modern network, Juniper® SD-WAN, driven by Mist AI™ has built-in security capabilities that are an inherent part of the architecture. In addition, service-based routing ensures that sessions are delivered based on identity and context to relevant parties following unified policies. This satisfies a key requirement of SASE, enabling modern cloud-centric digital businesses to provide secure access to users and devices anywhere.

When combined with security for LANs and cloud infrastructure via Security Service Edge (SSE) functionality, Juniper SD-WAN provides the basis for a full SASE solution. This includes SSE functionality such as Firewall as a Service (FWaaS), cloud access security broker (CASB), data loss prevention (DLP), and secure Web gateway (SWG), which enables enterprises to seamlessly transition to a cloud-delivered, single-stack architecture, securing their workforce wherever they are and delivering great user experiences.

Traditional Approaches Are Falling Short

Traditional approaches to security are no longer enough in the modern distributed workplace. As an example, the standard security model to protect users and data was to have firewalls at the perimeter. This led to having firewalls deployed at *any* perimeter, including the cloud, the data center, the desktop, or even the device. As BYOD and cloud services became increasingly prevalent, the perimeter became blurry, with user data residing in Software as a Service (SaaS) applications, mobile phones, laptops, and tablets. It's no longer possible to even define a physical perimeter, let alone apply consistent security policy at each of these enforcement points.

Backhauling traffic from many devices over VPNs to a data center is another method that has grown in usage during the continued rise of mobility. Using this approach, traffic is scrubbed by large, centralized firewalls before being forwarded to its destination. This requires large costly equipment at the data center to manage all the traffic, and it naturally increases latency due to backhauling. Defeating the cloud and SaaS model, this often results in poor user experience. To some extent, both of these methods are still being used, but they remain inadequate.

Secure Access Service Edge

In response to these trends, modern enterprises have been working with industry analysts to define requirements for new security capabilities. SASE was first defined in 2019 as an emerging architecture that would combine SD-WAN and network security into a single cloud-managed package.

©2022, Juniper Networks, Inc.

Since that time, SD-WAN's importance has been increasingly understood and validated: In How to Align SD-WAN Projects with SASE Initiatives (2022), Gartner continues to emphasize that SASE "converges SD-WAN solutions with cloud-delivered security services like Security Service Edge (SSE).[2] Essentially, this means combining SD-WAN capabilities with SSE functions such as FWaaS, CASB, DLP, and SWG, along with zero trust network access (ZTNA) to support the secure access needs of organizations in the cloud era.

Juniper's vision for SASE incorporates the capabilities of both SD-WAN and SSE.

SD-WAN
SASE
SSE

In the 2022 Gartner CISO Security Vendor Consolidation XDR & SASE Trends survey, Gartner predicts that by the end of 2023, "nearly 70% of organizations will have completed SASE projects.[3]

The Primacy of SD-WAN

The key starting point for SASE is SD-WAN, which ideally provides cloud-based management and security via software-based private connections between enterprise branches and cloud locations. From the onset (in 2019) of the SASE vision, the role of SD-WAN has been central to the SASE vision.

This is because SD-WAN functionality not only secures but simplifies the connectivity between users—who may be anywhere—and applications, which are hosted from clouds with increasing frequency, but also may be housed in a local data center. SD-WANs improve application performance and the user experience, and, by simplifying IT infrastructure, improve the operator experience as well.

Introducing AI-Driven SD-WAN

Recognizing that security must be fully integrated into the network, the Juniper® SD-WAN, driven by Mist AI™ solution (Figure 1) has built-in security capabilities that are an inherent part of the architecture. In addition, service-based routing ensures that sessions are delivered based on identity and context to relevant parties following unified policies. This ensures a key requirement of SASE: a modern cloud-centric digital business can provide secure access to users and devices wherever they are located.

[2] Gartner, How to Align SD-WAN Projects with SASE Initiatives, Bjarne Munch, Lisa Pierce, Craig Lawson, 18 April 2022

[3] Gartner Infographic, Top Trends in Cybersecurity 2022—Vendor Consolidation, Dionisio Zumerle, August 19, 2022

GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

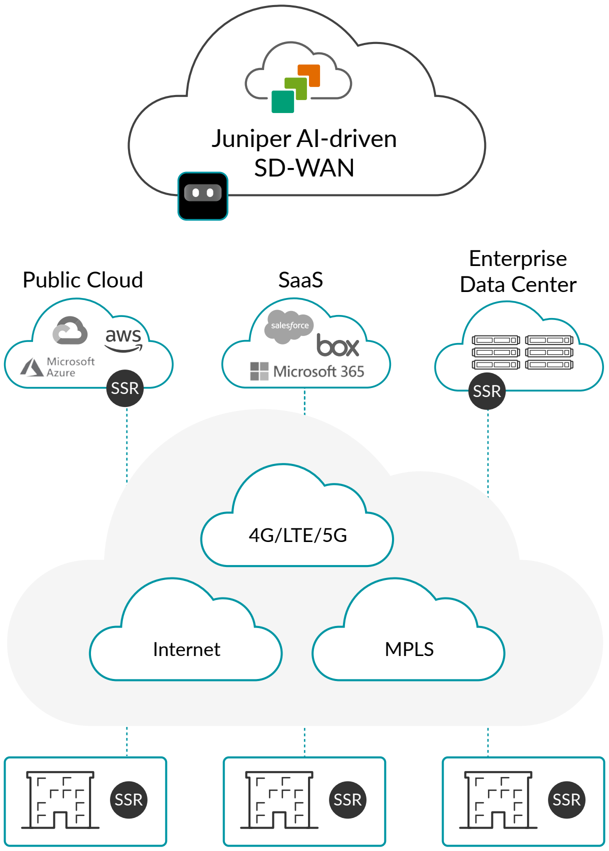

Figure 1: AI-driven SD-WAN supports any business type

A complete client-to-cloud solution, Juniper SD-WAN supports any branch size as well as large campus and data center environments. Public clouds and SaaS applications are accessible over any common WAN or Internet links.

Juniper SD-WAN is driven by Mist AI (for AI-based insights and resolution) and Juniper Session Smart™ Routing, which provides application-layer control so that critical applications receive priority treatment and guaranteed uptime based on session policies and network status. The Session Smart Routing fabric maintains full end-to-end context (state) of user sessions, services, and applications, as well as other dynamic workloads for a far more responsive network.

The solution scales to tens of thousands of sites while accelerating service deployment through centralized orchestration of global policies from a microservices cloud architecture and zero-touch provisioning (ZTP). The tunnel-free architecture enables up to a 30 to 50 percent reduction in bandwidth costs.

Juniper SD-WAN manages traffic on the session layer, thus ensuring that applications and users (with unpredictable devices in disparate locations) are all mapped correctly. This "deny-by-default" approach to applications, servers, and consumers bakes zero trust security into the SD-WAN fabric. Other facets of this zero trust approach include:

- Multihop authentication
- Full visibility into individual traffic flows to efficiently monitor end-to-end sessions, evaluate service quality, and troubleshoot problems in a tunnel-free architecture
- Enforced directionality and segmentation policies with zero trust access control

Network performance is optimized with Juniper Session Smart Routing's unique Secure Vector Routing protocol, which ensures user experiences aren't sacrificed as a result of needless double encryption and overhead. SVR provides the ability to collect, analyze, and act upon session and application data.

Juniper SD-WAN driven by Mist AI includes the industry's only Juniper Mist WAN Assurance functionality, which provides a self-driving and self-correcting network framework that includes:

- Real-time visibility into the WAN user experience by interpreting application health, link health, and network element health
- Automated identification and correction of gateway misconfigurations, faulty interfaces, or other network, security, or application issues
- Simplified Day 1 operations with intuitive QR claim code scanning and configuration templates for Session Smart Routers

This all leads to the highest quality user and operator experience. The Juniper AI-driven SD-WAN provides a self-driving network, identifying and acting on root causes of issues across IT domains and, automatically fixing or recommending actions. The solution provides fine-grained quality of service (QoS), subsecond failover, and lossless application delivery.

In a comprehensive TCO analysis, ACG Research has shown that the Juniper wired, wireless, and SD-WAN driven by Juniper Mist WAN Assurance and Mist AI reduces OpEx by 85% and decreases TCO by 28%.

An Ideal SASE Starting Point

Although SD-WAN is a cornerstone of SASE, some SD-WANs are more valuable than others in creating a SASE environment. The main advantage of Juniper SD-WAN is the deny-by-default approach to session access, providing a zero trust environment. Many other security features are built into Juniper SD-WAN as well (Figure 2).

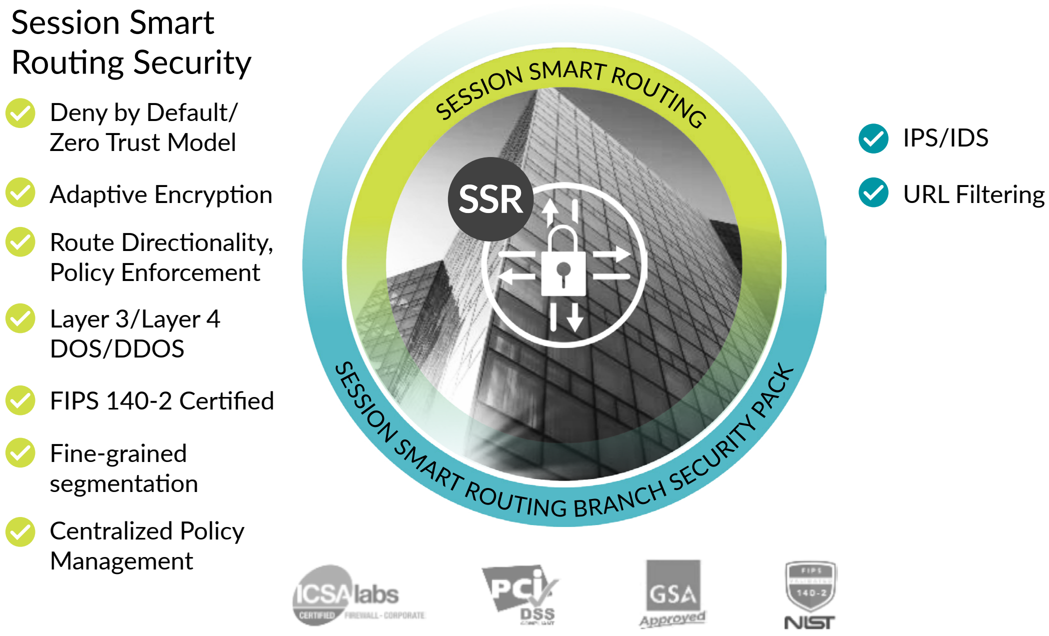
Session Smart Routing Security
✓ Deny by Default/ Zero Trust Model
✓ Adaptive Encryption
✓ Route Directionality, Policy Enforcement
✓ Layer 3/Layer 4 DOS/DDOS
✓ FIPS 140-2 Certified
✓ Fine-grained segmentation
✓ Centralized Policy Management
SESSION SMART ROUTING
SSR
SESSION SMART ROUTING BRANCH SECURITY PACK
✓ IPS/IDS
✓ URL Filtering
ICSA labs CERTIFIED FIREWALL - CORPORATE
PCI DSS
GSA Approved
FIPS 140-2 NIST

Figure 2: Secure SD-WAN with zero trust

SASE requires that network devices closest to users and their devices can dynamically provide security services by discovering endpoints and their privileges, and securing the traffic. The Juniper AI-driven SD-WAN has built-in capabilities to provide numerous security services from every router in the network. Furthermore, The Juniper Branch Security Pack contains intrusion detection and prevention systems (IDS/IPS) and URL filtering capabilities.

Session-Based and Service-Centric

Session Smart Routers provide the core routing functionality in the Juniper SD-WAN solution. Similar to upper-layer firewall operations, Session Smart Routers operate on sessions rather than individual packets. This enables the router to understand which users and services are allowed to initiate sessions and in which direction. An administrator can specify these sessions based on any given authentication criteria.

Juniper SD-WAN models the applications that users consume. Administrators describe the services within the network and the group(s) within the network allowed to access each application. This enables the network to route sessions to and from services only when both the users and the sessions are validated.

Policies associated with sessions may relate to security, encryption, authentication, QoS, loads, or other criteria. This can be hypersegmented to be individually customized per session. Any unauthorized session will be dropped as soon as traffic traverses the first router in the network.

Advanced Firewall Functionality

Juniper SD-WAN includes built-in corporate network firewall functions and provides policy-based policing and forwarding. Enterprises can provide differentiated security and services to every traffic flow.

- Session Smart Routers can encrypt/decrypt and authenticate any packet flowing through them. They support adaptive encryption to dynamically detect encrypted sessions and prevent double encryption.
- If no policy is associated with a session, the session will be dropped. This forces administrators to explicitly define policies for valid sessions.

If and when more SSE functionality is needed, enterprises can integrate with an SSE suite to achieve a complete SASE solution..

Completing SASE with SSE Functionality

For organizations seeking a full-stack SASE solution, Juniper offers a suite of Secure Services Edge (SSE) capabilities under unified security management with the Juniper Secure Edge (Figure 3).

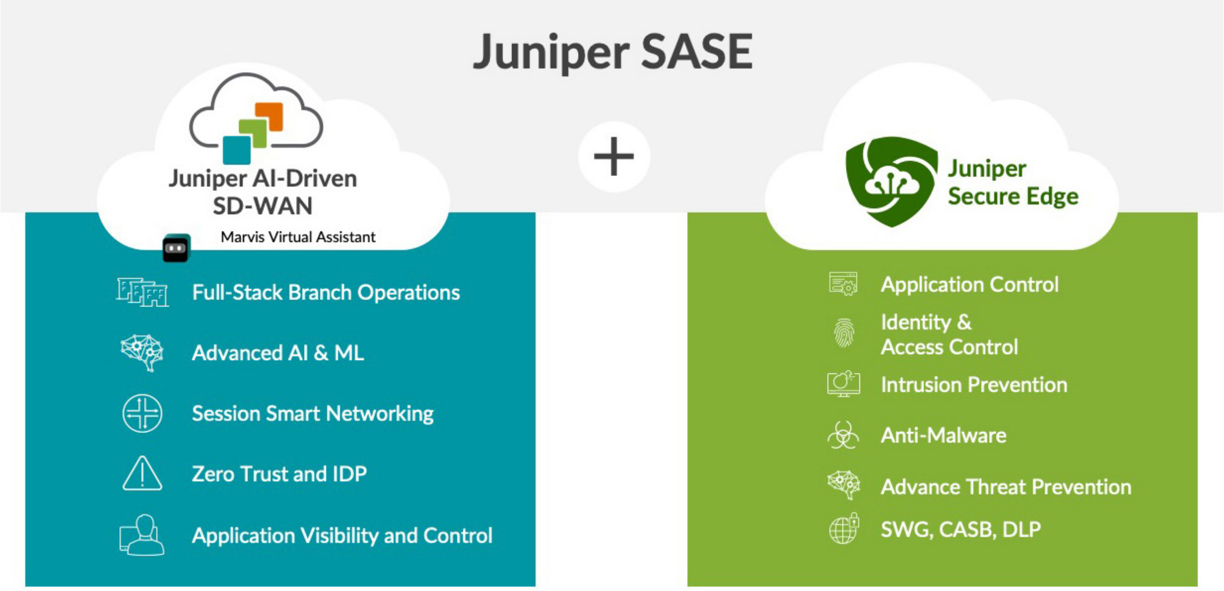

Figure 3: Juniper SASE combines Juniper SD-WAN with Juniper Secure Edge

When combined with Juniper SD-WAN, Juniper Secure Edge provides a best-in-class SASE solution (Figure 4).

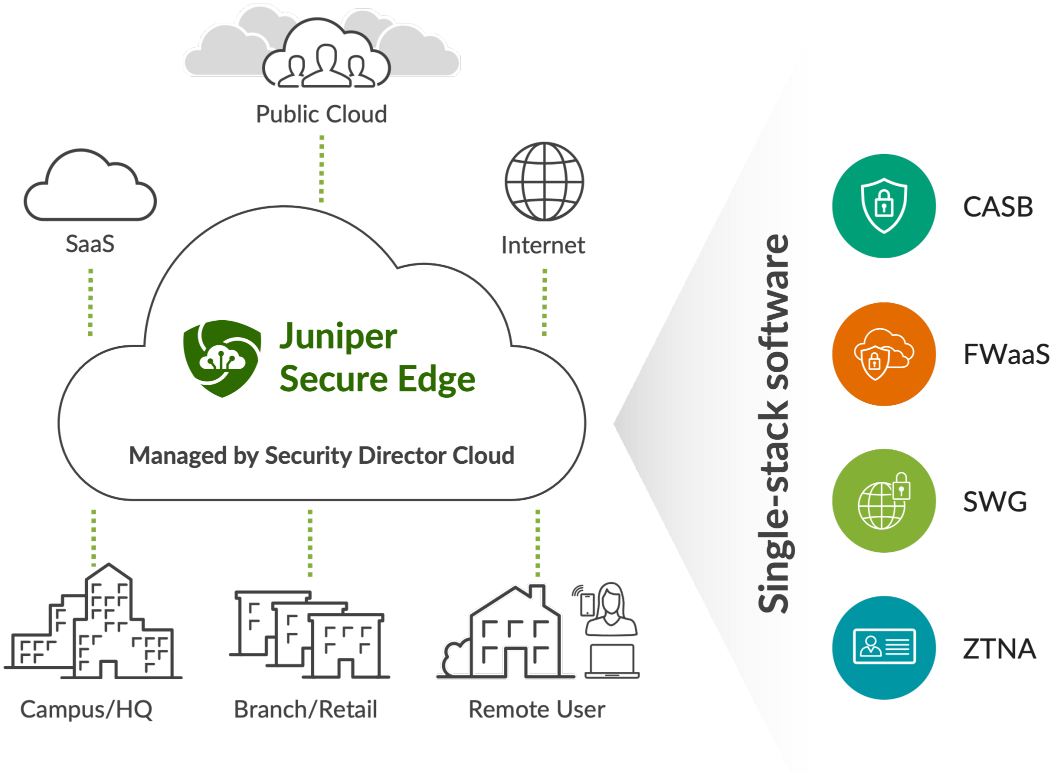

Figure 4: Juniper Secure Edge protects locations, functions, users, and devices

With Juniper Secure Edge, organizations can connect their users anywhere in the world directly to applications. They can accomplish this while effectively securing those connections—and therefore securing the applications themselves. The effect is to be able to scale out enterprise edge security enhancements at the desired pace. This could mean changes for sets of sites or groups of users, or could alternatively be implemented one site or user at a time.

Enterprises can seamlessly transition to a cloud-delivered, single-stack architecture. This empowers organizations to secure their workforce wherever they are. Users have fast, reliable, and secure access to the applications and resources they need, ensuring great user experiences.

Juniper Secure Edge includes:

- Firewall as a Service (FWaaS): Identifies applications and inspects traffic for exploits and malware with over 99.8 percent effectiveness. FWaaS is delivered via Juniper's managed cloud. CyberRatings assigned Juniper Networks vSRX Virtual Firewall the highest rating of "AAA" for threat protection, blocking 100% of exploits and evasions without a single false positive.
- Secure Web Gateway (SWG): Protects Web access by enforcing acceptable use policies and preventing web-borne threats. Juniper's SWG provides Web traffic control through granular URL-based policies, content inspection, and selective SSL decryption to protect against web-based attacks.
- Cloud Access Security Broker (CASB) and Data Loss Prevention (DLP): CASB discovers sanctioned and non-sanctioned SaaS applications in use and provides visibility and granular controls to ensure authorized access, actions, threat prevention, and compliance. DLP provides granular visibility and control over data housed in SaaS applications and prevents sensitive data from leaving your network either inadvertently or as part of an attack.
- Juniper Advanced Threat Prevention: Discovers zero-day malware and malicious connections, including botnets and command and control (C2), even when traffic cannot be decrypted. Enforces granular protection mechanisms, such as file quarantine and reduced access rights.

©2022, Juniper Networks, Inc.

Juniper SASE in Action

A Juniper SASE deployment highlighting this combined functionality is shown in Figure 5.

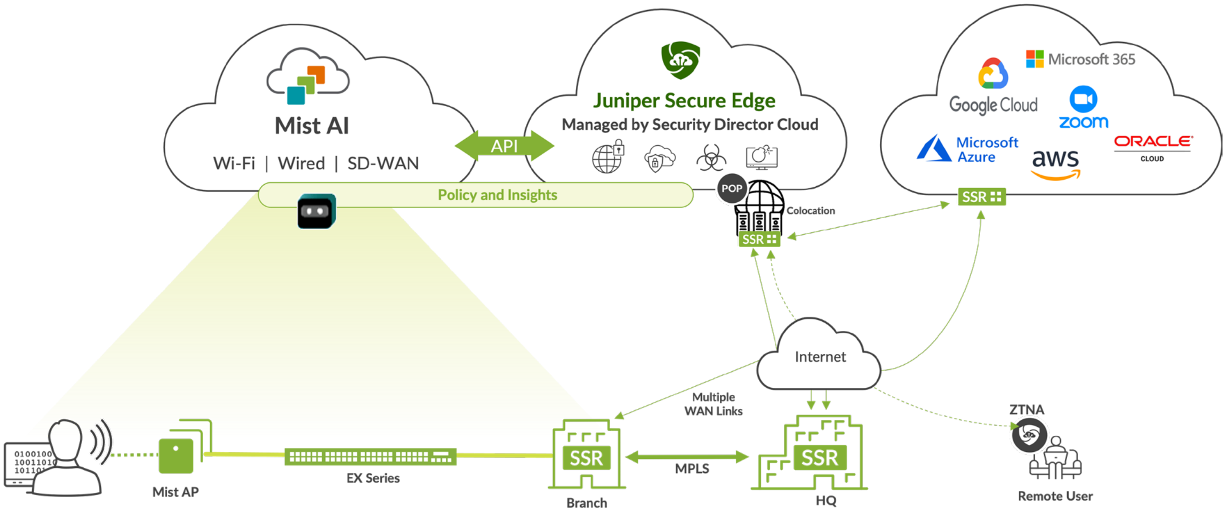

Figure 5: Juniper SASE in action

In this example, the solution from the branch includes multiple WAN links (for redundancy and/or load balancing). These WAN links may be broadband, MPLS, or LTE. Note that the Juniper Mist Cloud manages Session Smart Router nodes in all locations: branches, headquarters, data centers, and the cloud.

Traffic reaching the point of presence (POP) may be handled by any relevant SSE functionality in Juniper Secure Edge. For instance, SSE functionality will sometimes be required to secure remote users. Integrated through an API, Juniper SD-WAN and Juniper Secure Edge contain shared policies and insights that ensure secure access for all locations, clouds, users, and devices in the distributed enterprise. SD-WAN traffic is deny-by-default for zero trust security and is tunnel free for bandwidth optimization. Any unencrypted traffic is adaptively encrypted.

For brownfield deployments, or when customer-specific capabilities are needed for a particular network function, Juniper SD-WAN also integrates with third-party SSE solutions.

Conclusion

Traditional networking and security infrastructure is ill-suited to meet the needs of an increasingly distributed workforce. There has been a sharp rise in remote workers who need to securely and reliably access numerous public and private cloud services, and this has driven the industry to define and refine the requirements for SASE.

Enterprises of all sizes and in every industry recognize that SD-WAN is an essential foundational element for SASE, securing access to disparate locations and dispersed users. Juniper delivers an AI-driven SD-WAN that is tunnel-free and session-aware. Juniper SD-WAN provides deny-by-default access and adaptive encryption with bandwidth savings on the order of 30 to 50%.

When combined with security for LANs and cloud infrastructure via SSE functionality, Juniper SD-WAN provides the basis for a full SASE solution. Furthermore, Juniper provides SSE functionality such as FWaaS, CASB, DLP, and SWG to support the secure access needs of distributed organizations in the cloud era. The combined solution provides secure support for thousands of branches and cloud service edges, with integrated policy and insight management assuring excellent user and operator experiences.

Next Steps

For more information and assistance in starting or continuing your SASE journey with Juniper SD-WAN, contact your Juniper account representative.

©2022, Juniper Networks, Inc.

Resources

Web Pages

- AI-Driven SD-WAN
- Session Smart Router
- SASE
- Secure Edge
- Mist AI and Cloud

Solution Briefs and White Papers

- AI-driven SD-WAN Secures Today's Cloud-Era Networks
- AI-driven SD-WAN: Building Networks with Security at their Core
- Client to Cloud Assurance with an AI-driven Enterprise
- Session Smart Routing: How it Works
- SASE Buyer's Guide

Datasheets

- Session Smart Router
- WAN Assurance
- Secure Edge

Analyst and Press References

- ACG: Financial Benefits of the Juniper Networks AIOps Solutions
- Gartner: How to Align SD-WAN Projects with SASE Initiatives

Webinars

- Juniper Networks SASE (SD-WAN + SSE) Webinar and Demo | Juniper Networks US
- SASE Things: Don't Let An Alternate Dimension Take Over
- SASE Things: Take Control of your Universe
- SASE and Beyond: Juniper Webinar Featuring Gartner Expert

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.

JUNIPer NETWORKS | Driven by Experience™

APAC and EMEA Headquarters
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
Phone: +31.207.125.700
Fax: +31.207.125.701

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

Copyright 2022 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, Juniper, Junos, and other trademarks are registered trademarks of Juniper Networks, Inc. and/or its affiliates in the United States and other countries. Other names may be trademarks 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.

2000804-001-EN Oct 2022