JUNIPER NETWORKS | Driven by Experience™

AI-DRIVEN SD-WAN SECURES CLOUD-ERA NETWORKS

Modernize the network with inherent security, enhanced visibility, and simplified management

White Paper

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Despite the proliferation of techniques to secure, restrict, or segment the network, the number of security breaches, denial-of-service events, and other cyberattacks have grown ever more prevalent and sophisticated. All these factors have affected service delivery. In the modern cloud era, it is a constant battle to protect enterprise networks, intellectual property, and confidential information—while ensuring simple, safe user access.

By contrast, the Juniper® SD-WAN, driven by Mist™ AI, offers a unique approach to zero trust security and segmentation. It introduces a set of tools for network design intended to allow operators—both service providers and enterprises—to build an SD-WAN around the services it is meant to deliver.

Powered by Mist AI and the Juniper Session Smart™ Router, AI-Driven SD-WAN modernizes the network with inherent security, enhanced visibility, and simplified management.

AI-Driven SD-WAN delivers zero trust protection with integrated security, network isolation, segmentation, load balancing, and firewall functions. This tight control of the packet flow within the network is very powerful and can limit, and often eliminate, network attacks.

Introduction

Networks are inherently insecure because they pass network traffic by default. Broadcasts and default routing enable compromised devices to communicate with devices they should not be able to access.

As a result, network operators have grown accustomed to configuring complex sets of access control lists (ACLs) and deploying third-party hardware to gain functionality like firewalling, intrusion detection and protection services (IDS/IPS), load balancing, and traffic segmentation. These rely on tunneling technologies such as IPsec, Transport Layer Security (TLS) or Generic Routing Encapsulation (GRE), and they all add unnecessary complexity and overhead to the network.

Enterprises need a simpler and more secure SD-WAN that utilizes bandwidth efficiently and applies the power of AIOps for simpler operations and optimized user experiences. The Juniper AI-Driven SD-WAN, which is built on the Juniper Session Smart Router and managed by Mist AI, fulfills this need.

The Session Smart Router has built-in security capabilities that are an inherent part of the product architecture. In addition, service-based routing, which is natively supported by the Session Smart Router, ensures that sessions are delivered based on identity and context to relevant parties based on real-time policies. This ensures that a modern cloud-centric digital business can provide secure access to users, devices, and applications anywhere.

Juniper Mist cloud offers a single management platform for Session Smart Routers, Juniper High-Performance Access Points, and Juniper Networks EX Series Ethernet Switches. Optimal user experiences are assured using Service Level Experiences (SLE) that are measured and fine-tuned under Mist AI.

AI-Driven SD-WAN: Inherently Secure

AI-Driven SD-WAN, a key pillar of the AI-Driven Enterprise, facilitates a Secure Access Service Edge (SASE) network with deny-by-default routing, policy-based forwarding, policing, and built-in corporate network firewall functions. The solution enables end-to-end segmentation, allowing enterprises to segregate and provide differentiated security and services to every traffic flow.

The default behavior of AI-Driven SD-WAN is to treat and apply security controls to sessions, regardless of whether the session has originated internally or externally. Keeping data safe and accessible by modernizing the network with inherent security, enhanced visibility, and simplified management is at the heart of Session Smart Routing.

The architecture begins with a unique set of key principles and capabilities that transform the network into an asset for enterprises that need to compete in today's data-driven landscape. Traffic is only accepted on the network if it is defined by a prespecified set of users, applications, and devices. This is verified at every hop.

Benefits of the Session Smart Router architecture include:

- **Deny-by-default access policies**: Traffic must belong to predefined networks and applications to be accepted onto this network.
- **Hop-by-hop authentication**: This is ensured at each hop.
- **Distributed stateful firewall**: A flexible approach to zero trust that is enforced network-wide.
- **Route directionality**: Bidirectional traffic patterns are preestablished and enforced.
- **Centralized policy management**: Predefined policies are defined between users, devices, applications, and services.

Deny-by-Default Access Policy

The Session Smart Router allows network architects to describe how their network will be used in a whole new way. It starts by associating networks (groups of users and their address ranges) with the applications and services that they use: examples include CRM and ERP systems, as well as mail, voice, and Web resources. Access to these services is granted (or not) based on an organization's policies (Figure 1).

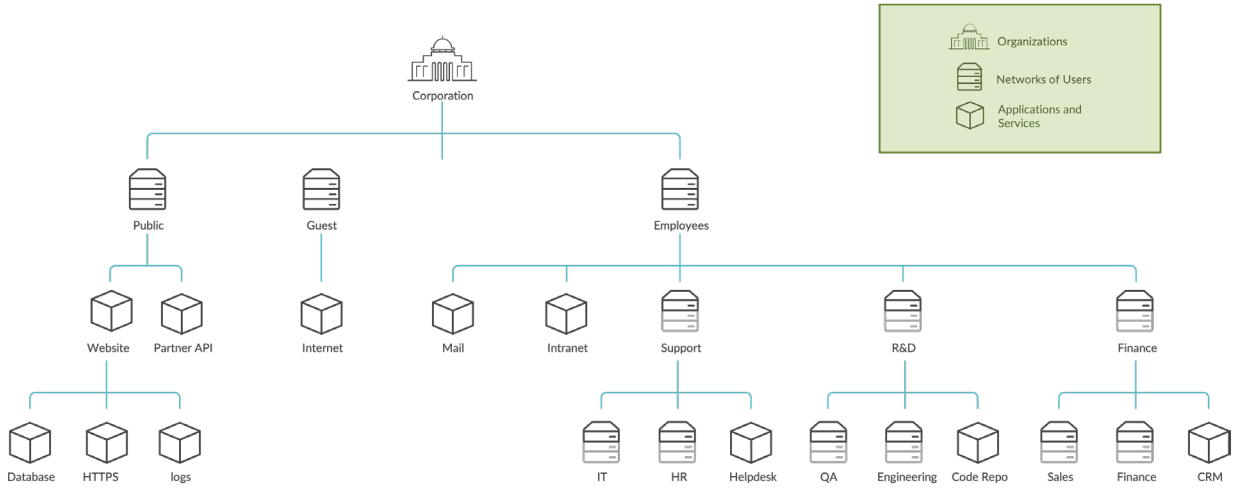

Figure 1: Networks, services and applications are defined for each organization.

Administrators define the networks that use applications and services, granting or denying access to those applications for members of the various teams. These users and applications are shared among every Session Smart Router within the organizational domain. Security properties such as authentication and encryption keys are also shared. This ensures that network resources are offered only to those permitted to use them.

As sessions are processed in AI-Driven SD-WAN, users and their devices work within their predefined route determination, segmentation, classification, policy, and many other capabilities (Figure 2).

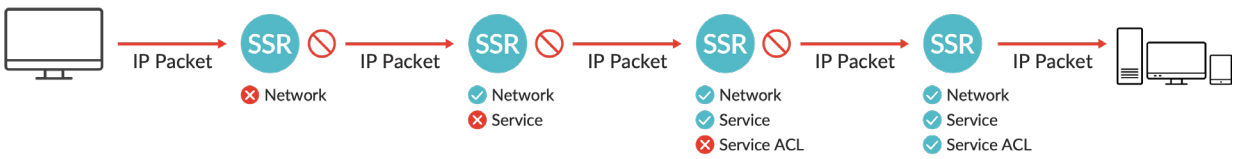

Figure 2: AI-Driven SD-WAN has a deny by default access policy

When a Session Smart Router receives a packet, it first checks whether the packet belongs to an accepted network:

- If not, the packet will be dropped.
- If so, the next check is to verify whether it is destined for an application that the user has permission to access. If not, the packet will be dropped.
- If the packet is allowed to access the service, the packet will be forwarded to the next hop towards the destination.

This tight control of the packet flow within the network greatly reduces the risk of network attacks and data breaches.

Hop-by-Hop Authentication and Adaptive Encryption

A primary requirement of zero trust security is to support policy-based inter-router traffic encryption and authentication. See the Session Smart Routing Datasheet for details on encryption, authentication, and relevant standards.

Metadata

As part of the flow setup process, the system exchanges metadata in the first packet. Signing and optionally encrypting the metadata exchanged in the first packet creates a secure fabric that is reserved for its own exclusive use (Figure 3).

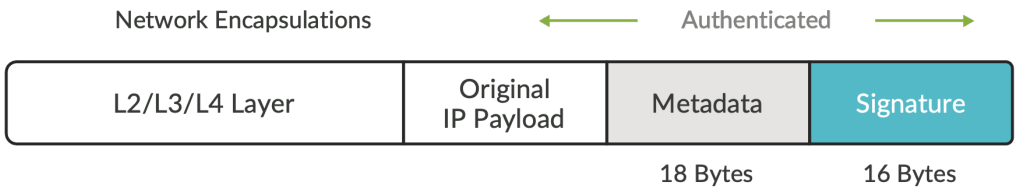

Figure 3: Metadata influences traffic handling in Session Smart Routing

Effectively, the metadata ensures that all traffic will stay with the Session Smart Routing fabric. Metadata information includes the desired applications for the client and all associated devices. The original source and destination addresses are maintained, along with all of the policies and controls that influence the session.

For a detailed walkthrough of how metadata influences secure bidirectional traffic handling in an AI-Driven SD-WAN, see Session Smart Routing: How it Works.

Table 1 shows the encryption capabilities and the architectural benefits of AI-Driven SD-WAN.

Table 1: Comparison on AI-Driven SD-WAN, TLS, and IPsec

	AI-Driven SD-WAN	TLS	IPsec
Strong encryption	Yes	Yes	Yes
Strong authentication	Yes	Yes	Yes
Per-packet overhead	Minimal: 32-48 bytes	More: 52 bytes	Most: 78 bytes
Operates without control protocol	Yes	Yes	No Requires IKE
Simple key exchange (automatic generation a nd distribution)	Yes	No Many control packet exchanges	No Many control packet exchanges
Easy to configure and manage	Yes	No	No
Easy to deploy and troubleshoot	Yes	No	No
Does not require certificates	Yes	No	No
Stateless encryption	Yes	No	No

Table 1 compares the AI-Driven SD-WAN encryption/per-packet authentication schema with IPsec and TLS 1.3. AI-Driven SD-WAN provides FIPS 140-2 level encryption and per-packet authentication with minimal overhead (32-48 bytes) compared to TLS (52 bytes) and IPsec (78 bytes).

Also, since encryption and authentication keys are automatically generated and distributed, AI-driven SD-WAN eliminates the need for complicated key exchange protocols like IKEv1 and IKEv2 required by IPsec or PKIX -based X.509 digital certificates.

Because of the session-oriented nature of the Session Smart Routers, they can detect whether the traffic is already encrypted using TLS/HTTPS or by IPsec, while performing encryption of the application. If the application traffic is already encrypted using IPsec or TLS, an optional setting called adaptive encryption ensures that the router will not re-encrypt the packet.

Adaptive encryption eliminates the overhead associated with double encryption, which is a significant issue in networks where IPsec is used between branch offices or data centers for interconnections and multisite VPNs. Since voice and video traffic are latency and jitter sensitive, double encryption with IPsec can have an undesirable impact on application performance and business operations.

Distributed Stateful Network Firewall

Most enterprises still implement perimeter-based security, which uses standalone firewall devices at the edge of the network. Firewall technology heavily relies on ACLs and VLANs to control access to various segments of the enterprise network. As the network grows, the number of required ACLs and VLANs for access control grows exponentially.

This makes the firewall ACL rules unmanageable and error prone, exposing the enterprise to various security threats and network attacks. Even when enterprises move from perimeter-based security to a microsegmentation approach, firewall devices are still deployed at the edge of every segment, having the same complexities associated with ACLs.

By contrast, AI-Driven SD-WAN behaves as a session-aware firewall, eliminating the need for a global ACL and error-prone configurations. The AI-Driven SD-WAN solution provides complete L2, L3, and L4 session-aware capabilities through a standard firewall, which eliminates the need for standalone firewalls.

Only valid networks of users and devices are allowed to access applications and services. This simplifies configurations while maintaining a high-security standard in terms of access control (Figure 4).

Figure 4: AI-Driven SD-WAN provides a multiple security functions.

There is additional security functionality for intrusion detection and prevention and URL filtering; this is provided by the Advanced Security Pack. Furthermore, third-party cloud networking security services are available through Secure Edge Connectors, which allow connections to other cloud security applications, such as Juniper Secure Edge or third-party solutions.

Route Directionality

Most of the legitimate traffic on an IP network has packets that flow bidirectionally, creating a session between two endpoints. Session Smart sessions consist of two flows, one in the forward direction and one in the reverse direction. This creates predictable route directionality.

After a session becomes established in one direction, subsequent packets in the session transit through the two unidirectional flows that are instantiated. Thus, in a session controlled by the AI-Driven SD-WAN solution, all flows have path symmetry: flows in the forward and reverse direction for a session follow the same path through the network for traffic symmetry across the network.

Traffic symmetry allows for optimal traffic steering and path selection, preventing latency by avoiding nonoptimal paths. Directionality becomes extremely useful for analysis and troubleshooting of network traffic, and greatly simplifies the entire SD-WAN through the administration of routes based on directional sessions and traffic symmetry.

There are strong security implications as well. When directionality is attached to session creation, it prevents rogue programs on a server or device from sending sensitive data to the external world.

For example, if a policy is configured to allow session creation from the client to the server only, AI-Driven SD-WAN will not allow a server to initiate a session back to the client or to the external world. This effectively eliminates most sophisticated security attacks.

Centralized Policy Management

The AI-Driven SD-WAN solution provides centralized policy management, administration, provisioning, monitoring, and analytics through Juniper Mist cloud, via a single-pane-of-glass view for all routers running in the enterprise network (Figure 5).

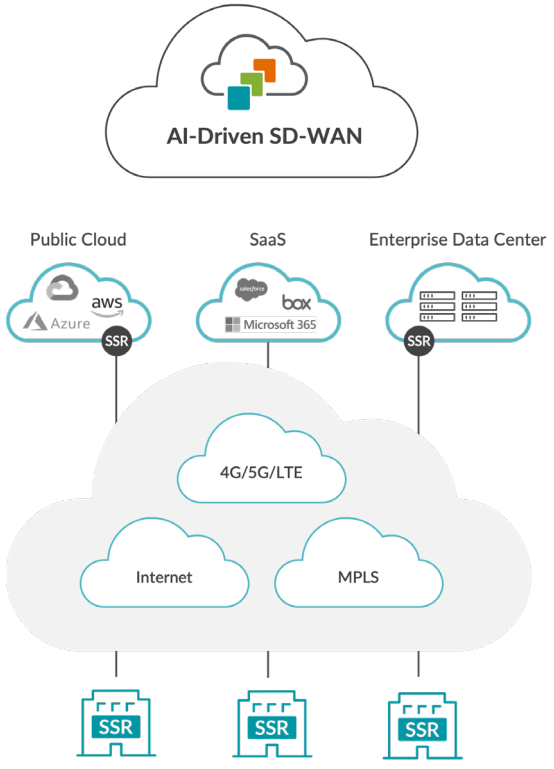

Figure 5: AI-Driven SD-WAN

Since the definitions of the applications and services are global within an organization, defined policies are globally applied to all the routers under an organization, thus eliminating the need for defining custom policies per Session Smart Router. At the same time, the Session Smart Router has the ability to perform service-level policy enforcement, thus making all policies context-specific. This level of application awareness and control ensures optimized user experiences.

WAN Assurance

Juniper Mist WAN Assurance, a cloud-based service, brings AI-powered automation and service levels to the AI-Driven SD-WAN. Using the power of Mist AI and Marvis Virtual Network Assistant, WAN Assurance provides AIOps capabilities that ensure customers can understand and improve their users' experience across the SD-WAN (Figure 6).

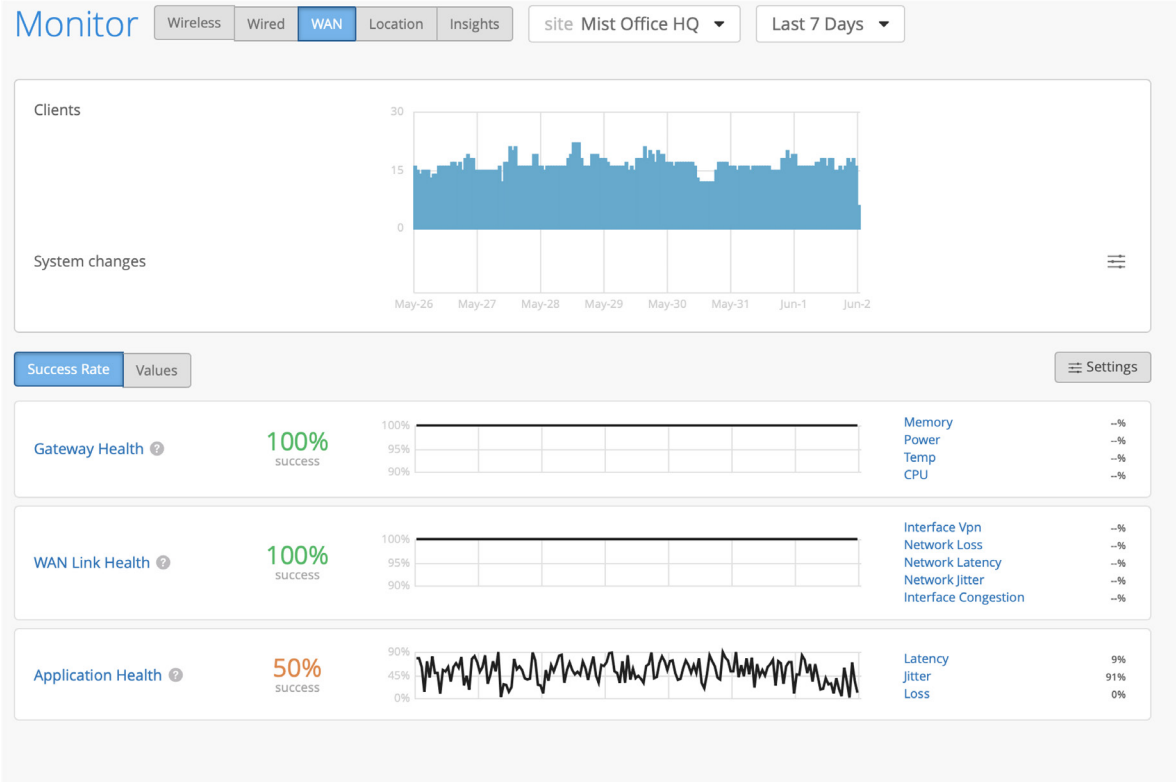

Figure 6: Juniper Mist WAN Assurance tracks gateway, link, and application health.

The SLEs for WAN Assurance are Gateway Health, WAN Link Health and Application Health. Each of these has Classifiers shown at the right of the image, to help pinpoint why there might be an issue with one of the SLEs. In Figure 6, jitter appears to be the main reason for issues with application experience.

For more on SLEs and Classifiers, see Implementing Branch Networks for AI-Driven Enterprise Customers. Also see the Guided Setup for Juniper Mist WAN Assurance.

Hypersegmentation

Traditional network segmentation is zone-based, separating users into trusted and untrusted zones and providing many security layers within that network or subnetwork. All the users, devices, and servers within a given zone can freely talk with each other. In a LAN environment, this would equate to sharing an Ethernet broadcast domain. To traverse zones means going through a firewall, which requires an explicit policy to allow the IP traffic through. Firewalls control the so-called "north/south" movement of network traffic into and out of the zone and allow "any-to-any" communication within a segment.

Some vendors "solve" these inefficiencies with overlay networks based on virtual extensible LAN (VXLAN) and network virtualization using GRE (NVGRE), and partnerships with third parties to implement security and network segmentation. Since the overlay networking technology is not inherently secure, this approach to microsegmentation depends on third-party firewalls and Deep Packet Inspection (DPI) devices for securing the boundary of the network segments. This is expensive and complicates the overall solution. It is difficult to implement and maintain, as well as costly because it has considerable per-packet overhead.

As an alternative to these approaches, Session Smart Routers segment networks down to single endpoints and services associated with those endpoints, while providing a named-based hierarchy, enabling easy and effective administration and enforcement of security policies. This approach, called hypersegmentation, is the cleanest and most efficient approach to zero trust networking security (Figure 7).

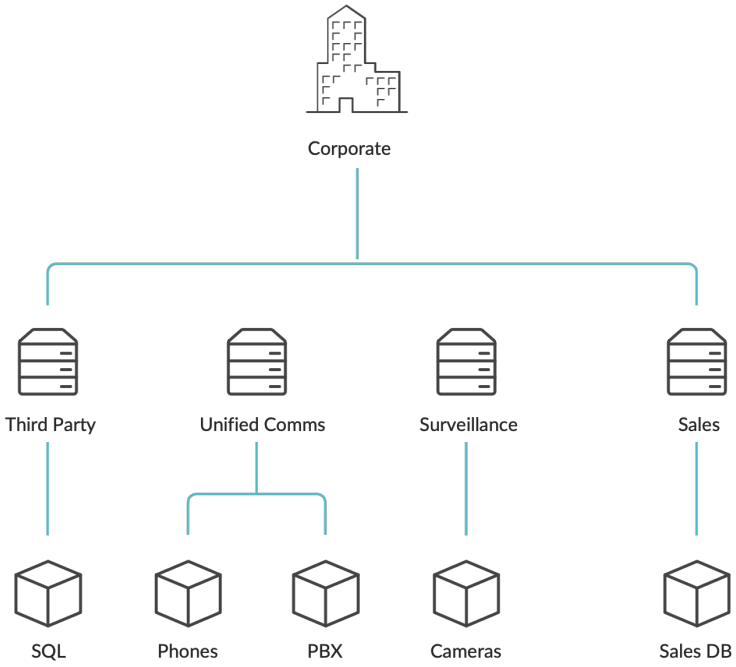

Figure 7: AI-Driven SD-WAN Hypersegmentation

Hypersegmentation is a powerful and unique technology that enables organizations to avoid expensive and complicated overlays and simplify management, while also enhancing security. AI-Driven SD-WAN provides hypersegmentation of the network based on sessions, services, applications, and networks.

In this way, the solution treats every session as a segment and grants the ability to apply unique security rules (such as URL filtering to control access to content), firewall, and DPI at the session level.

The following sections describe the major advantages of hypersegmentation.

Fine-Grained

Whereas microsegmentation aligns segmentation with individual applications, hypersegmentation aligns with entire sessions, thus providing complete isolation for a deeper level of security. Hypersegmentation is based on how traffic is classified across the enterprise branch, data center, and into the cloud.

All traffic is classified at each Smart Session Router based on a combination of local network characteristics such as IP address/prefix or VLAN, and application/session type identification. The classifications define access control and membership for each segment along with the corresponding services belonging to this segment. Unless explicitly configured, users belonging to one department will not be allowed to access services belonging to other departments.

Tunnel Free

Traditional approaches to segmentation depend on the outdated perimeter security model, constructing network segments with complex firewall rules, and static VLAN or tunnel configurations. AI-Driven SD-WAN provides isolated virtual layer networks using Secure Vector Routing.

Furthermore, network services (such as Layer 3, ACL, stateful firewall, QoS, load balancing, and URL filtering) are natively integrated into the solution, and distributed to every branch, every data center or public cloud, and every hypervisor. This simplification means firewall-specific configurations, and error-prone VLAN or complex tunnel configurations, are no longer needed.

End to End

Hypersegmentation allows segmentation to stretch from data center to data center, data center workload to the branch, and ultimately to devices, treating multiple networks and network islands as a single unified fabric, allowing seamless end-to-end segmentation.

Conclusion

The AI-Driven SD-WAN approach to zero trust security and segmentation introduces a whole new set of tools for network design intended to allow operators to build the network around the applications and services it is meant to deliver (rather than around the network itself). The ability to partition service availability is one of the key ways that AI-Driven SD-WAN ensures flexibility and efficiency with zero trust security. Users and their devices are continually accounted for, along with applications and their state. This is powerful and unique among SD-WAN solutions.

Next Steps

For more information and assistance in starting or continuing an AI-Driven SD-WAN journey, contact your Juniper account representative or inquire about a Juniper AI-Driven Enterprise managed service offering through your trusted provider.

In many cases, a managed service can reduce time and costs as IT resources are supplied on demand. The approach can lead to greater assurance of necessary knowledge and experience, and smoother integration with other network and cloud services.

You can also see firsthand how to perform many of these tasks by setting up an account at manage.mist.com and following the tutorials. Ask your account representative for help to get started.

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.

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

2000765-002-EN March 2023