JUNIPER NETWORKS | Driven by Experience™

White Paper

# AI-DRIVEN SD-WAN SECURES TODAY'S CLOUD-ERA NETWORKS

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

# TABLE OF CONTENTS

Executive Summary ..... 3

Introduction ..... 3

AI-driven SD-WAN ..... 4

- Deny-by-Default Access Policy ..... 5
- Hop-by-Hop Authentication and Adaptive Encryption ..... 6
- Distributed Stateful Network Firewall ..... 9
- Route Directionality ..... 10
- Secure Routing Fabric ..... 10
- Centralized Policy Management ..... 11
- Juniper Mist WAN Assurance ..... 12

Hypersegmentation ..... 12

- Fine-Grained ..... 13
- Directional ..... 13
- Overlay/Tunnel Free ..... 14
- End to End ..... 14

Conclusion ..... 14

About Juniper Networks ..... 14

# EXECUTIVE SUMMARY

Today's networks are built using foundational technology that has changed very little since the inception of the routed IP network in the 1990s. ASIC-based switches and routers were designed to facilitate an "any-to-any" model for packet exchange, where computers can freely communicate with each other using paths built hop-by-hop by the networking equipment between them.

Despite the proliferation of various 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, and this has affected service delivery. In the cloud era, it is a constant struggle to protect enterprise networks, intellectual property, and customers' confidential information.

This document is for network and security architects who want to better understand zero trust security and the Juniper® AI-driven SD-WAN solution. Utilizing AI-driven SD-WAN, powered by the Juniper Session Smart Router (SSR), modernizes the network with inherent security, enhanced visibility, and simplified management. Its approach to zero trust security and segmentation is unique, introducing a new set of tools for network design intended to allow operators to build the network around the services it is meant to deliver. 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 in some cases eliminate, network attacks.

## Introduction

Networks are inherently insecure because they pass network traffic by default. Broadcasts and default routing enable compromised devices to talk to other devices on the network. An access control list (ACL) is then used to restrict where traffic can go. As a result, network operators have grown accustomed to configuring complex sets of ACLs, deploying third-party hardware to gain functionality like firewalling, intrusion detection service (IDS)/intrusion prevention system (IPS), load balancing, and segmenting traffic using overlay technologies like Virtual Extensible LAN (VXLAN), IPsec, and network virtualization using GRE (NVGRE), or any number of tunneling techniques.

The Juniper AI-driven SD-WAN solution is comprised of the Juniper Session Smart Router (SSR), and managed by either the Juniper Session Smart Conductor or the Juniper Mist AI and Cloud:

- The SSR 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 SSR, 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 and devices anywhere.
- The Session Smart Conductor provides centralized policy management, administration, provisioning, monitoring, and analytics with a single-pane-of-glass view of the network.
- The Juniper Mist AI and Cloud offers a single management platform for Session Smart Routers, Juniper Mist Access Points, and Juniper EX switches.

AI-driven SD-WAN enables end-to-end user and application control by providing true identity-based routing, and it extends fine-grained control based on the user identity and the user context. This allows the user context to be extended beyond the endpoint, all the way to the enterprise network, thus providing an end-to-end segmented, authenticated, and authorized network.

AI-driven SD-WAN is also FIPS-140-2 certified, enables a Zero Trust Architecture (NIST publication 800-207) and 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.

For a true zero trust security network, a network must be built at a minimum with the following capabilities:

- Session awareness
- Hop-by-hop authentication
- Adaptive encryption
- Deny-by-default access policies
- Distributed stateful firewall
- Route directionality
- Secure routing fabric
- Centralized policy management
- Hypersegmentation

## AI-driven SD-WAN

According to the Computer Security Institute, 60 to 80 percent of network misuse incidents originate from inside the network.[1] Often, the severity of these attacks is intensified because traditional firewalls and IDS are ineffective against attacks that originate internally. The default behavior of the AI-driven SD-WAN solution is to treat and apply security controls to sessions, regardless of whether the session has originated internally or externally. Modernizing the network with inherent security, enhanced visibility, and simplified management is at the heart of Session Smart Routing, which is designed to keep data safe, and is simple and flexible enough to make sure the data is accessible. It all 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.

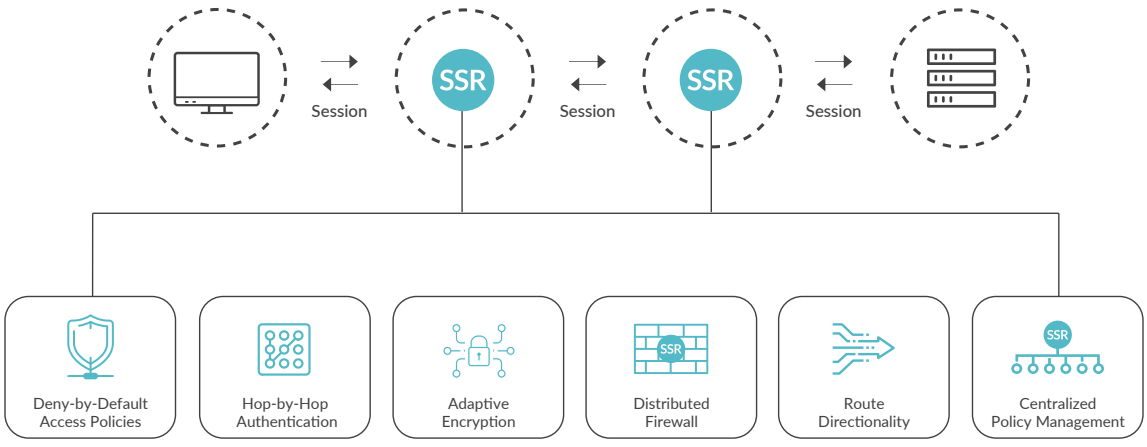


*Figure 1: Capabilities of the AI-driven SD-WAN solution*

[1] https://www.techrepublic.com/article/myth-or-not-most-security-breaches-originate-internally

### Deny-by-Default Access Policy

The SSR uses an innovative data model that lets network architects describe how their network will be used in a whole new way. It starts with the bases of the network, which are the services employees use; for example, the CRM system, ERP system, mail, voice, and Web resources. Access to these services is granted based on tenancy: each tenant in the data model represents a collection of users and their devices that share common access and security policies. Unlike zone-based schemes, tenancy is applied and enforced at every SSR instance, network-wide, with tenant policies "stretching" across the network.

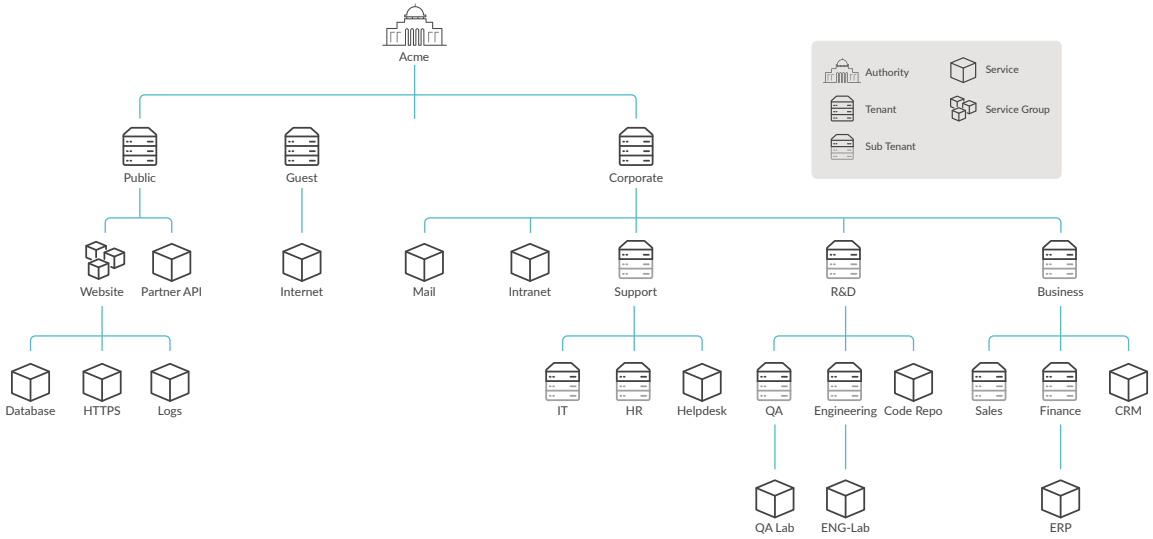


*Figure 2: Access to network services is based on tenancy*

Administrators define the tenants (user populations) that use network services. Using an intuitive, text-based, associative language, administrators grant or deny access to those services for members of the various tenants on the network. These tenants and services are shared among every SSR within an authority, or administrative domain, along with security properties such as authentication and encryption keys. This ensures that network resources are offered only to those permitted to use them. Under the hood, these tenant and service definitions govern the construction of each router information database (RIB) and forwarding information database (FIB).

A tenant functions as a network partition used to group services together. As sessions are processed through the solution, the tenant becomes an important construct for route determination, segmentation, classification, policy, and many other capabilities.

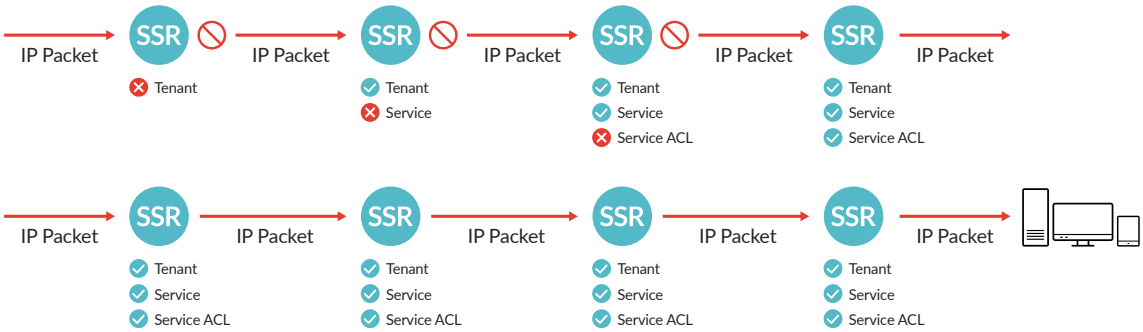


*Figure 3: Deny-by-default access policy*

Unlike a traditional router, which has the default policy of "allow-by-default," the SSR follows the principle of "deny-by-default." This means that when a packet hits the router, the router first checks whether the packet belongs to a tenant. If the packet does not belong to a tenant, it will be dropped. If the packet belongs to a tenant, the next check is to verify whether it is destined for a service, which the tenant is allowed to access. If the destination of the packet does not correspond to any service within the tenant, the packet will be dropped. Finally, if the tenant is allowed to access the service, the packet will be forwarded to the next hop towards the destination. While performing these checks with every packet, the SSR maintains the traffic rate to match with the line rate.

With a deny-by-default approach, unless an enterprise explicitly enables a session to traverse through the network, the SSR will drop all the packets belonging to the session. This tight control of the packet flow within the network reduces the risk of network attacks and data breaches.

### Hop-by-Hop Authentication and Adaptive Encryption

The SSR is built on the principles of zero trust security. One of the primary requirements of zero trust security is to support policy-based inter-router traffic encryption and authentication. Every packet exchange between SSRs is authenticated and encrypted by default using HMAC-SHA256-128 and AES256, respectively.

As part of the flow setup process, the system exchanges metadata in the first packet. The metadata exchanged is signed using HMAC-SHA256-128. Optionally, the metadata can be encrypted using AES256. Signing and optionally encrypting the metadata exchanged in the first packet creates a secure fabric in which the system's routing fabric is reserved for its own exclusive use. This helps defend against insiders and eavesdroppers.

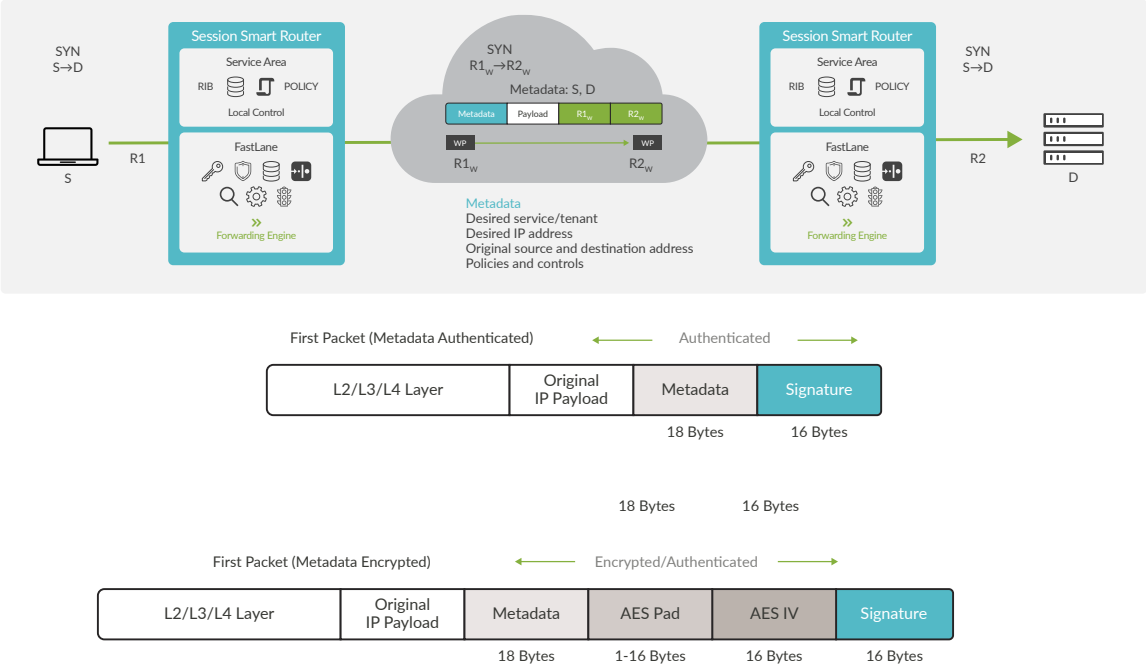


*Figure 4: Authentication and adaptive encryption*

The keys for encryption and per-packet authentication are dynamically generated by the solution at boot time and are securely stored. Per-session encryption is supported between every SSR and protected using FIPS 140-2 based AES256 encryption and per-packet authentication based on the HMAC-SHA256-128 algorithm.

Encryption is done in a stateless manner by explicitly carrying an initialization vector in each packet. The initialization vector is generated using the FIPS140-2 Deterministic Random Bit Generator (DRBG)[2] method. The DRBG method of generating an initialization vector allows the solution to generate a true random number, thus providing complete protection from man-in-the-middle and replay attacks.

[2] https://en.wikipedia.org/wiki/Dual_EC_DRBG

Table 1: Comparison of AI-driven SD-WAN, IPsec and TLS

| | IPsec | TLS | AI-driven SD-WAN |
|---|---|---|---|
| Strong encryption (AES256) | ✔ | ✔ | ✔ |
| Strong per-packet authentication (HMAC-SHA256-128) | ✔ | ✔ | ✔ |
| Low per-packet overhead | ✘ 78 Bytes | ✔ 52 Bytes | ✔ 32-48 Bytes |
| Does not require a control protocol | ✘ Requires IKEv1/IKEv2 | ✔ | ✔ |
| Simple key exchange | ✘ Can require up to 14 control packet exchange for key generation | ✘ Can require up to 14 control packet exchange for key generation | ✔ Keys are automatically generated and distributed |
| Easy to configure and manage | ✘ | ✘ | ✔ |
| Easy to deploy and troubleshoot | ✘ | ✘ | ✔ |
| Does not require certificate/PKIX support | ✘ | ✘ | ✔ |
| Stateless encryption | ✘ | ✘ | ✔ |

The table above compares the AI-driven SD-WAN encryption/per-packet authentication schema with IPsec and TLS 1.2. As shown in the table, AI-driven SD-WAN provides FIPS 140-2 level encryption and per-packet authentication with minimum overhead (32-48 bytes) compared to IPsec (78 bytes) and TLS (52 bytes). Also, since encryption and authentication keys are automatically generated and distributed, the solution eliminates the need for complicated key exchange protocols like IKEv1 and IKEv2 required by IPsec or PKIX[3] based X.509 digital certificates.

Because of the session-oriented nature of the SSR, routers 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, the router will not re-encrypt the packet. This is called adaptive encryption. 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 interconnect and multisite VPNs. Since voice and video traffic are latency and jitter sensitive, double encryption with IPsec can have an undesirable impact on business operations.

In short, AI-driven SD-WAN provides a simpler, more cost-effective FIPS 140-2 compliant encryption and authentication mechanism compared to what is provided by IPsec and TLS. Also, the adaptive encryption

mechanism provided by this solution eliminates the risk of fragmentation and double encryption of a packet, thereby minimizing latency and jitter, as well as cost.

[3] https://datatracker.ietf.org/doc/html/rfc5280

### Distributed Stateful Network Firewall

Most current enterprises 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 and overall manageability.

The AI-driven SD-WAN solution behaves as a session-aware firewall, eliminating the need for a global ACL list and error-prone configurations, with access control tied to services with a tenant. By default, only members of a tenant are allowed to access its services within, thereby minimizing the complexity of configurations, while

maintaining a high security standard in terms of access control. When a non-member wants to access the services of a tenant, the access control policy is specified within the service. This leads to an access control rule that is very context-specific and pertinent to the service.

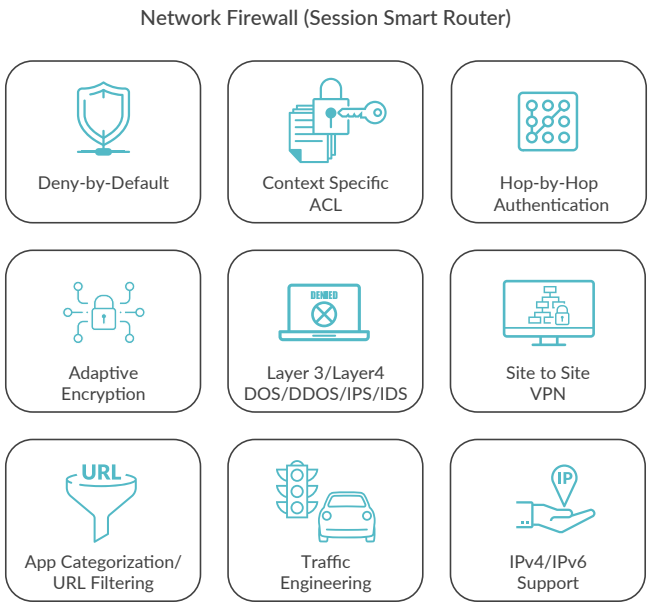


*Figure 5: AI-driven SD-WAN distributed stateful firewall capabilities*

In addition to tenant-based segmentation and access control, the AI-driven SD-WAN solution provides complete L2/L3/L4 session-aware capabilities through a standard firewall, which eliminates the need for standalone firewalls. The AI-driven SD-WAN solution also includes sophisticated traffic engineering and URL filtering.

### Route Directionality

There are a few profound implications of the session-oriented nature of the SSR. Through the administration of routes based on directional sessions and traffic symmetry management, the network itself becomes much simpler.

Most of the legitimate traffic on an IP network has packets that flow bidirectionally, creating a session between two endpoints. Sessions have directionality in that they are initiated from one endpoint (e.g., a client) to another endpoint or endpoints (e.g., a server). They consist of two flows, one in the forward direction and one in the reverse direction. After a session becomes established in one direction, subsequent packets in the session transit through two unidirectional flows that are instantiated. In traditional switching and routing infrastructures, forward and reverse flows may take asymmetric paths through the network. In a session controlled by the AI-driven SD-WAN solution, the flows have path symmetry. AI-driven SD-WAN is built with an orientation around the sessions that exist between endpoints over an IP network.

This is the first step in delivering simplicity afforded by the administration of routes in the network. It contrasts from traditional destination-based routing, where routes for the forward and reverse paths must be expressed throughout the network in order for any traffic to occur. With session orientation, routes can be expressed in terms of the directional sessions, which automatically include the two unidirectional flows that comprise a given session. This combines the functions of a router and a stateful firewall to simplify networks and improve security.

Flows in the forward and reverse direction for a session follow the same path through the network for traffic symmetry across the network. This becomes extremely useful for analysis and troubleshooting of network traffic. Traffic symmetry also allows for optimal traffic steering and path selection.

### Secure Routing Fabric

With built-in zero trust security capabilities, the SSR allows an enterprise to build security controls into every segment of the network to create a secure routing fabric. In traditional routed networks, because of the allow-by-default policy, most of the packets are transported without any controls. In a network built around the SSR using a deny-by-default policy, the overall role of the network shifts from transporting all the packets across the network, to transporting only those packets that are verified to be safe and properly encrypted, and which are legitimately required to run the enterprise.

Instead of relying on ACL lists and rules to determine which traffic may not be transported (and transporting everything else), the SSR transports only traffic which has been expressly green-lighted. This built in security makes the network fabric and routing algorithms high effective tools in creating a simple, cost-effective and distributed defense against increasing security threats.

### Centralized Policy Management

The AI-driven SD-WAN solution provides centralized policy management, administration, provisioning, monitoring, and analytics through the Session Smart Conductor or the Mist Cloud, via a single-pane-of-glass view for all routers running in the enterprise network.

With traditional firewall devices, the difficulty with managing policy grows exponentially as the network expands. A powerful and flexible feature on the SSR is the ability to perform service-level policy enforcement, thus making policies context-specific. This level of application awareness and control leads to optimized user experiences.

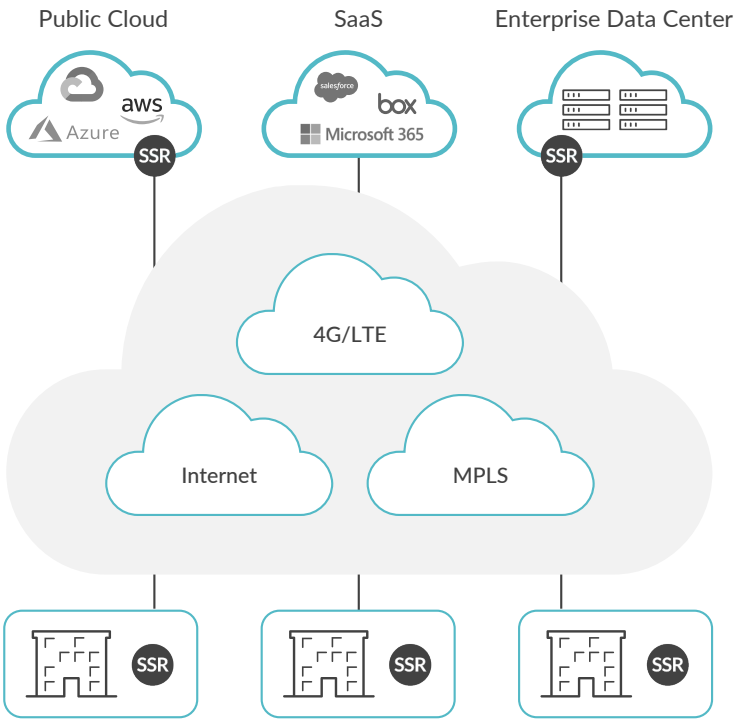


*Figure 6: AI-Driven SD-WAN*

Since the definition of the services is global within an authority, policies defined within the services are globally applied to all the routers under an authority, thus eliminating the need for defining custom policies per router.

The access control rules within a service can be specified in terms of IP prefix or by making use of qualified service name. A qualified service name provides a mechanism to address the resource using a hierarchical Uniform Resource Identifier (URI) name instead of an IP address. The qualified service name concept minimizes the errors that can be caused while defining access policies in terms of IP prefix and ports.


*Figure 7: Qualified service name*

### Juniper Mist WAN Assurance

AI-driven SD-WAN provides Juniper Mist WAN Assurance, a cloud service that brings AI-powered automation and service levels to the SD-WAN solution. Driven by 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 9*).

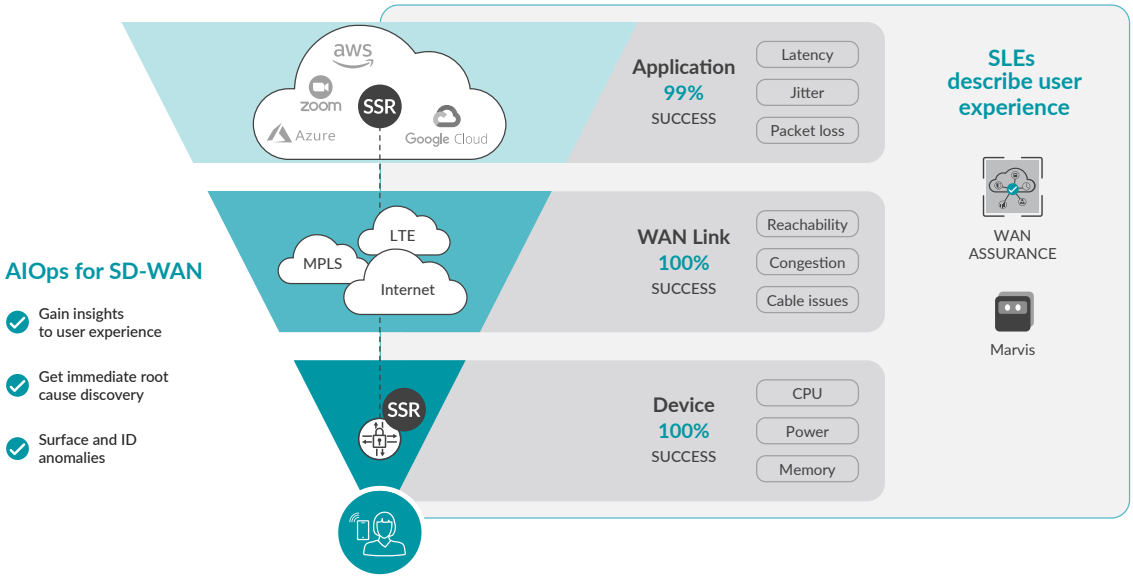


*Figure 8: WAN Assurance*

This allows customers to gain insights to user experiences, obtain immediate root cause discovery, and detect anomalies in devices, links and applications.

## Hypersegmentation

Juniper Networks has developed a way of segmenting networks down to single endpoints and services on those endpoints, while providing a named-based hierarchy, enabling easy and effective administration and enforcement of security policies.

Traditional network segmentation is zone-based, defining users into trusted and untrusted zones and providing many security layers within that network or subnetwork. All the users, computers, 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 go between zones requires going through a firewall, which requires an explicit policy to allow the IP traffic through. The 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.

Additionally, the concept of microsegmentation, marketed by many vendors, relies on overlay networks (based on VXLAN and NVGRE) and partnerships with third parties to implement security and network segmentation. Given the fact that the overlay networking technology is not inherently secure, microsegmentation depends on third-party firewalls and DPI devices for securing the boundary of the network segments. This painted on security makes the overall solution complicated, expensive, and difficult to manage. Also, since overlay technology is oriented around tunneling and multicast technologies, it is difficult to implement and maintain, as well as costly because it has considerable per-packet overhead.

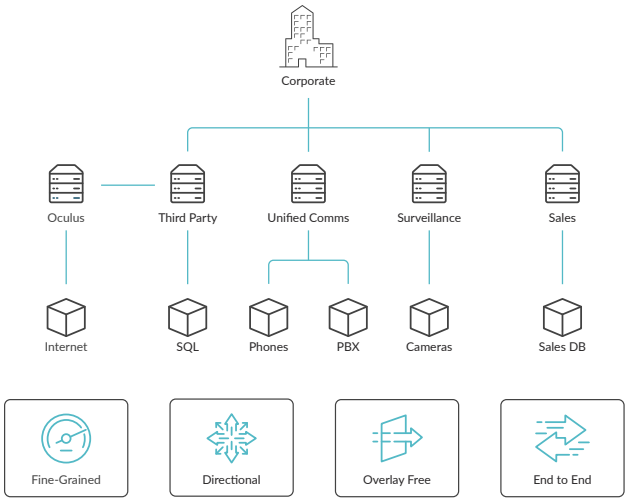


*Figure 9: AI-driven SD-WAN hypersegmentation*

AI-driven SD-WAN has security built in from the ground up, providing hypersegmentation of the network based on sessions, services, and tenants. The session-oriented nature of this solution allows the platform to treat every session like a segment and grants the ability to apply unique security rules (such as URL filtering to control access to content), firewall, denial-of-service (DOS)/distributed DOS (DDOS) prevention, and DPI at every session level. The resulting hypersegmentation becomes a very powerful and unique technology that enables organizations to avoid expensive and complicated overlays and simplify management, while also enhancing security.

The following sections describe the major components of hypersegmentation.

### Fine-Grained

Microsegmentation aligns segmentation with applications. However, hypersegmentation takes segmentation a step further to align with sessions, thus providing complete session-level isolation for a deeper level of security.

All segmentation with hypersegmentation is based on how traffic is classified across the enterprise branch, data center, and into the cloud. All traffic is classified at each SSR based on a combination of

local network characteristics such as IP address/prefix or VLAN, and application/session type identification. The classifications are grouped by tenants that define access control and membership for each segment along with the corresponding services belonging to this segment. Unless explicitly configured, members belonging to one tenant will not be allowed to access services belonging to other tenants.

### Directional

When directionality is attached to the session creation, it prevents rogue programs on the server from sending sensitive data to the external world, effectively eliminating many of the high-profile attacks seen in the recent past. Session initialization is tightly controlled within each segment and attaches directionality to the created session. This means that 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, thus attaching strict directionality (a vector) to the session creation process.

### Overlay/Tunnel Free

Traditional approaches to segmentation depend on an outdated perimeter security model, constructing network segments with complex firewall rules, and static VLAN or tunnel configurations. AI-driven SD-WAN provides isolated virtual L3 networks as a function of Secure Vector Routing (SVR), the routing protocol behind the SSR. Furthermore, network services (L3, ACL, stateful firewall, QoS, load balancing, and URL filtering) are natively integrated into the solution, distributed to every branch, every data center, and every hypervisor. This improved simplification means firewall-specific configurations, and error-prone VLAN or complex tunnel configurations, are no longer needed.

### End to End

Since microsegmentation makes use of multiple tunneling technologies (VXLAN in data center and IPsec between data centers), achieving end-to-end segmentation is very complex and difficult to manage.

Because no overlays are required, 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

For decades, routed and overlay networks have been designed around an increasing number of prefixes, tags, labels, identifiers, and encapsulations that are only significant to the networks and their topology. The AI-driven SD-WAN approach to zero trust security and segmentation is entirely different, introducing a whole new set of tools for network design intended to allow operators to build the network around the services it is meant to deliver, rather than around the network itself. This enables the routing and policies of the network to be expressed in terms that allow for semantic meaning to be applied to businesses and applications, not network topology.

The ability to partition service availability—afforded by the network using tenants—is one of the many ways that AI-driven SD-WAN is fixing the network by fixing the router. Tenants are present in the very forwarding tables and packet pipelines of the AI-driven SD-WAN solution, making them a foundational component of the routed network itself.

## About Juniper Networks

Juniper Networks is 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. Additional information can be found at Juniper Networks (www.juniper.net) or connect with Juniper on 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**
**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**

JUNIPER NETWORKS | Driven by Experience™