Session Intelligence in a Tunnel-Free SD-WAN

How Session Smart Networking Overcomes the Limitations of Tunnels

White Paper

Table of Contents

Executive Summary

Network administrators and engineers implement software-defined WANs (SD-WANs) to support distributed enterprises of all sizes. These SD-WANs are generally built using tunneling technologies such as IPsec, Generic Routing Encapsulation (GRE), or Virtual Extensible LAN (VXLAN).

Tunnel-based networking provides a measure of security for SD-WANs, but greatly increases complexity and wastes network resources. This leads to unpredictable performance and poor experiences.

A tunnel-free, session-intelligent SD-WAN improves user and operator experience for all applications, whether real time or asynchronous. Using **Juniper® Session Smart™ Networking**, *Juniper* **SD-WAN, driven by Mist AI™**, *is higher performing, higher scale, more secure, and simpler to operate than tunnel-based SD-WANs.*

Additionally, **Juniper Mist™ WAN Assurance** *with Session Smart Networking provides dramatically better experiences for network users and operators.*

Introduction

Tunnel-based networking arose from a need for better security in WANs and the Internet. To handle a booming demand for connectivity, private routed networks were built stateless and connectionless, delivering rising waves of traffic to worldwide destinations. Under these massive workloads, handling security at the network edges was the better option.

As public networks were increasingly used for high-value business applications, they needed more security built into the routing fabric itself. Tunneling protocols were developed for this purpose. Most notably, IPsec was developed to authenticate and encrypt packets for secure transmission across an IP network.

As software-defined networking (with its rapid development compared to creating purpose-built hardware) and later SD-WAN grew, IPsec proved to be a cost-effective way to securely handle traffic. IPsec was especially useful in dynamic multipath environments where organizations, user groups, and applications have both asynchronous (such as database access) and real time (such as telephony) traffic.

IPsec tunnels provided virtualization so that SD-WANs could handle larger and more abstract multisite, multicloud connectivity. However, the proliferation of these tunnels caused problems with operational complexity and bandwidth inefficiencies.

Tradeoffs with Tunnel-Based Networking

Tunnels fulfill security requirements with encryption and authentication, and provide a measure of tamper resistance with integrity checks. Standardization in tunneling protocols—especially IPsec but also GRE and VXLAN—ensures compatibility in heterogenous networks. Tunnels are versatile and support a range of applications.

However, these benefits come at a cost. The major tradeoffs with tunnel-based networking are shown in Table 1.

Table 1: Tradeoffs in Tunnel-Based Networking

Advantages	Disadvantages
Encryption ensures that even if bad actors intercept the data, they cannot read or understand its contents.	**Performance reduction** is 30-40% or more due to overhead.
Authentication ensures that only authorized devices can be part of a connection.	**Heavy encapsulation** forces smaller payload and less goodput.
Tamper resistance due to integrity checks prevents payload modification.	Tunnel management is overly **complex**.
Device compatibility and OS interoperability and independence is possible.	**Compatibility issues** exist across vendor implementations
A range of applications and services are supported.	**Quality can be limited**, especially with real-time video communications

The additional overhead from encapsulation is a major reason for the performance reduction in tunnel-based networks. As packets must fit into a specified Maximum Transmission Unit (MTU) size, the extra encapsulation forces a smaller payload per packet. Lower performance can be especially noticeable with high-bandwidth applications or resource-limited devices.

Tunnels also require numerous encryption algorithms and authentication methods. They are often implemented with keys for further security, and managing key infrastructure can be very complex in large deployments.

Furthermore, there are compatibility issues between different vendor implementations, even when using a standardized tunneling protocol. Tunnels can carry many individual sessions and yet these appear as one large session to the network.

Proper traffic classification is very difficult in these circumstances. Only by engineering traffic tunnel-by-tunnel can you make improvements to the user's experience, but even these improvements are limited, since individual applications are embedded within the tunnels.

Rise of SD-WANs and Continued Use of Tunnels

SD-WANs are well suited to modern business practices such as cloud computing, video conferencing, and remote work—all of which are pushing WANs to their limit. SD-WANs are more agile than traditional WANs, and make setting up new applications and services faster and easier.

While SD-WANs help with complexity, most are surprisingly unstable, partly through their reliance on tunnels. Each tunnel establishes a direct connection between two endpoints, like a company's headquarters and branch stores. Establishing tunnels between every site in a network can take a long time and easily become complicated.

In terms of SD-WAN scale, topology restrictions are often the most significant limitation: a hub and spoke topology is needed to avoid the complexity of managing an "n-squared" number of tunnels between all sites. This topology hampers real-time media going from branch to branch (Figure 1).

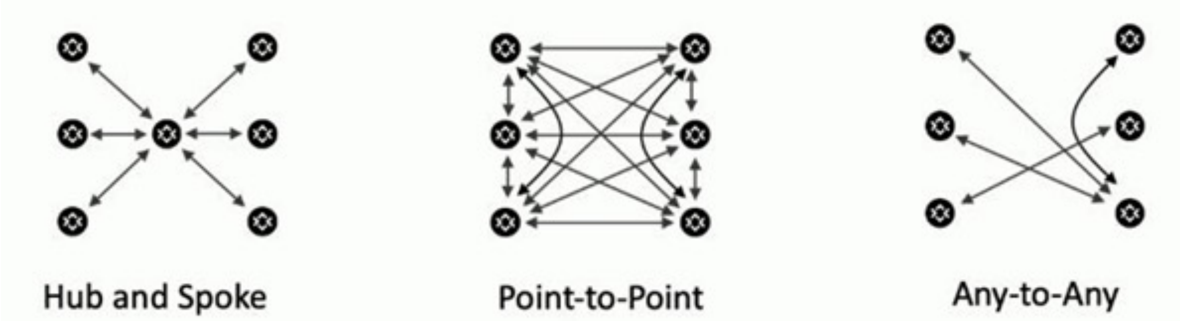

Figure 1: Topology limitations with tunnels, solved with Session Intelligence

The inefficient pathways due to extra hops in the hub-and-spoke topology add enough latency to make video calls unusable for many enterprise teams. An alternative would be point-to-point networking, which does not scale well and is difficult to manage.

An any-to-any topology, created for each session, circumvents these problems and provides a predictable, optimal path. This topology is much easier to implement without the overhead of managing tunnels.

Fragmentation is also an issue. Upon entry to a tunnel, if a packet is larger than can be supported, it is split into multiple packets, and reassembled on the other side. This takes processing power, memory, and CPU resources (Figure 2).

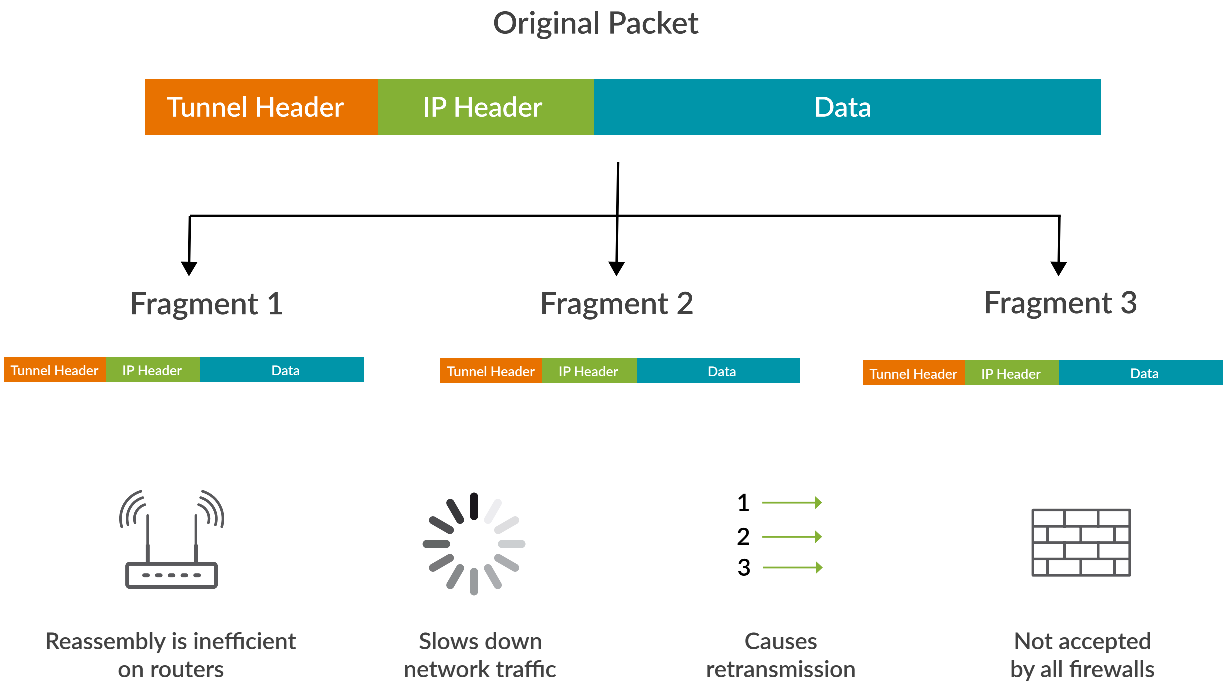

Figure 2: Fragmentation and reassembly issues

Along with this inefficient, costly reassembly, fragments are often lost and have to be resent. The increased transmission time results in lower throughput, limited scale, and a poor user experience. Furthermore, firewalls block out-of-sequence, non-initial fragments, leading to further drops and retransmissions.

More information on these two issues can be found in this white paper from ACG Research. Tunnels have other issues, particularly as they relate to SD-WANs. These include the lack of application visibility and the inefficiency of double encryption.

Juniper SD-WAN driven by Mist AI

Recognizing an opportunity to improve the experience for both operators and users, Juniper set out to build a better SD-WAN. Juniper's tunnel-free approach brings the advantages of session intelligence to SD-WAN routing, improving upon tunnel-based protocols, while delivering data integrity, encryption, and authentication.

Throughput Gains

One obvious advantage that Juniper SD-WAN, driven by Mist AI, provides is seen in the throughput gains by removing the overhead of tunnel headers, and replacing them with a more effective and lightweight design for a major increase in user payload (goodput) transmitted (Figure 3).

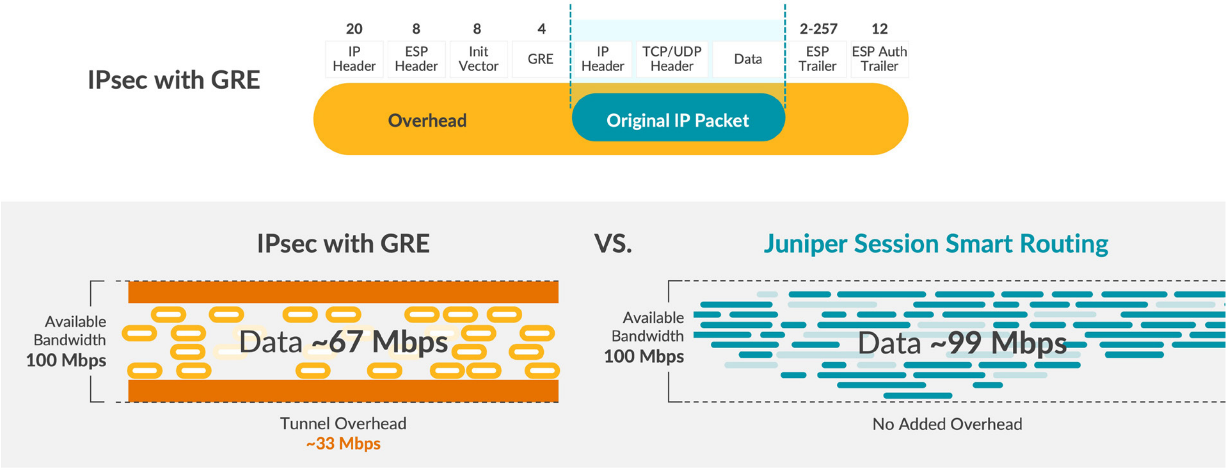

Figure 3: Wasted Bandwidth with IPsec and GRE

By not requiring tunnels, there is a 30% to 40% savings over IPsec and VXLAN-based networking schemes. The bandwidth usage can vary depending on the applications. Packet size is also a factor; for instance, for small voice packets, the savings can be closer to 100%.

Session Smart Advantages

Instead of using tunnels, the Juniper Session Smart Router, which powers Juniper SD-WAN, embeds a small metadata cookie into the first packet of a symmetric bidirectional connection that is needed for session establishment. The process uses waypoints to guide sessions across network paths. Juniper Session Smart Networking surpasses traditional network security with a zero-trust deny-by-default routing model: no session is permitted without explicit policies that allow it.[1]

Session Smart Networking emerged via a core principle taken from telephony: a user initiates a call, a receiver picks it up, and this constitutes a session. This is exactly how users and applications connect: session intelligence provides application awareness and adds assurances for each individual user’s experience. These assurances come in the form of guaranteed failover and QoS policies that are enforced on a per-user basis.

Conversely, in tunnel-based architectures, the quality of service (or experience) is only gauged—and can only be acted upon—at the tunnel level. This means that all applications within a tunnel are treated the same. However, within a tunnel, applications often have different requirements and may perform poorly for different reasons.

Thus, in a tunnel-based environment, much less value is gained by changing QoS settings for attributes such as latency, jitter, and loss across (for instance) Microsoft 365, an in-house database, and a video telephony application. Adjustments for one of these applications may in fact worsen the performance of another. A tunnel-based SD-WAN cannot take action on a per-application, per-user basis, and thus cannot prevent allowing traffic that's interfering with an application's performance.

[1] This is fully described in the Internet Draft for Secure Vector Routing and in Session Smart Routing – How it Works.

Session Smart Networking, on the other hand, provides greater, more granular visibility into each application. The difference is shown in Figure 4.

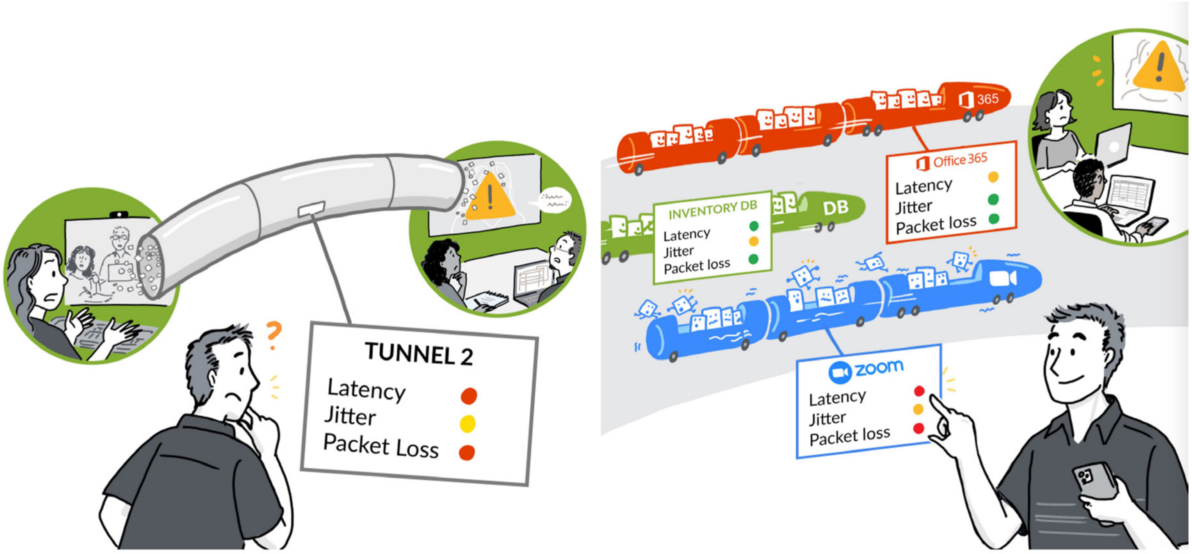

Figure 4: Operating on Sessions Rather than Tunnels

Application visibility and control are far more adjustable in this environment, ensuring the highest possible performance for all applications.

Combining Session Smart with Mist AI

As discussed previously, the tunnel-free nature of Session Smart Networking enables more granular visibility into network traffic. This enhanced visibility enables the router to collect richer telemetry. With Juniper Mist WAN Assurance, this rich telemetry is fed to the Mist AI engine, which provides actionable insights into network health.

The combination of Session Smart's rich telemetry with Mist AI's actionable insights (based on this data) is extremely powerful.

WAN Assurance uncovers root cause issues—such as application problems or slow server responses—that impact performance on the network. The telemetry provided by Session Smart improves the quality of these insights, helping IT operators find and remediate problems before they impact end-user experience.

Summary of Benefits

In addition to the benefits of combining AI with Session Smart, Session Smart Networking provides many other advantages.

Within an enterprise, sessions can scale to very large numbers. For example, any (or even most) of thousands of employees may be connected to internal databases, cloud stores, video and telephony applications, chat applications, browsers, intranet portals, or non-workrelated applications. If all or most of these applications are bundled into a single tunnel, it is impossible to detect and improve quality of experience in the applications. Session Smart Networking provides orders of magnitude higher scale in terms of sessions.

Furthermore, overall application performance can actually be many times faster, since retransmissions of dropped or out-of-sequence packets further slows applications. Due to this reduction of retransmissions, customers have seen as much as a 900% improvement in application performance.[2]

In the rare case that minimal fragmentation occurs, Session Smart Networking utilizes metadata signaling to instruct a receiver as to how to reconstitute fragmented traffic. The removal of MTU issues along the path ensures higher performance delivery.

Other differences are outlined in Table 2.

Table 2: Session Smart Networking versus Tunnel-Based SD-WAN

Tunnel-Free Session Intelligence	Tunnel-Based SD-WANs
Scales to as many as **millions of sessions**	Scales only to **thousands of sessions**
Flexible on-demand mesh architecture leading to efficient connections	**Forces a hub-and-spoke** architecture leading to tromboning of traffic
No overhead after first packet	**Consumes much more bandwidth**
Fragmentation is minimal and rare due to the lack of extra encapsulation that a tunnel might cause	Leads to **fragmentation** that causes poor performance
Rapid failover over heterogenous networks	**Failover deficiencies**; long tunnel setup time or unnecessary backup tunnels
Embraces security with hypersegmentation	**Bypasses security** by obscuring flows
Highly simplified key handling is totally managed by the system—with one key per session	Needs a **separate key management** infrastructure (e.g., PKI) using rotations and a certificate authority
Encryption in always available, yet there is no double encryption	**Encryption is low** and sometimes redundant

Prevention of double encryption occurs due to the Adaptive Encryption option, which identifies encrypted traffic and provides security for non-encrypted traffic by encrypting it through the Session Smart Router.

[2] See Next Generation Oil and Gas Networks Accelerate Digital Transformation.

Conclusion

Juniper SD-WAN, driven by Mist AI, and with Session Smart Networking, creates a tunnel-free, session-intelligent SD-WAN that improves user and operator experience for all applications, whether real time or asynchronous. Juniper AI-Driven SD-WAN powered by Session Smart is higher performing, higher scale, more secure, and simpler to operate than tunnel-based SD-WANs.

Advantages are in the areas of bandwidth and complexity reduction, avoidance of fragmentation and double encryption, zero trust security, simplicity of operations and rapid, reliable failover.

Further benefits are realized by feeding the rich telemetry of Session Smart Networking into the Mist AI engine. With WAN Assurance, IT gets actionable insights into WAN network health that vastly reduces troubleshooting time, thus improving user and operator experiences.

Resources

Videos

- Simplified: AI-Driven SD-WAN with Session Smart
- Session Smart Technology Overview (SVR)
- Dare to Compare: Juniper SD-Branch - Tunnel-Free SD-WAN

White Papers and Solution Briefs

- ACG Research: Tunnel-Bases Versus Tunnel-Free SD-WAN
- Session Smart Routing: How it Works
- Client to Cloud Assurance with an AI-Driven Enterprise

Infographic Content

- Eight Reasons to Go Tunnel-Free
- Is your Network Suffering from "Badput?"

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.

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