FEDERAL ORGANIZATIONS NEED A MISSION-FIRST NETWORK

Build an agile, resilient, secure network fabric to support offensive and defensive operations

Challenge

Warfighting increasingly relies on secure undeniable connectivity. As the nation's adversaries target critical infrastructure, joint forces must be able to continue net-enabled combat and operations in the face of overburdened infrastructure, difficult environments, determined adversaries, and insider threats.

Solution

Juniper's mission-first network, anchored on the Juniper Session Smart Router, enables organizations to adapt rapidly, providing the agility, resiliency, and security needed to support offensive and defensive missions, protect critical infrastructure, and ensure reliable communications under adverse conditions, with unprecedented simplicity and operational efficiency.

Benefits

- *Create a self-driving network that rapidly translates the intent of mission planners into network configuration*
- *Ensure mission-critical application delivery and communications over an ultra-resilient network fabric*
- *Run anywhere and use any type of IP connectivity with 100% software, on-premises solution*
- *Embed Zero Trust security into network fabric, repelling and avoiding attacks in real time*

Cyberwarfare has been described as the future of conflict between nations, whether that action is attacking another nation's critical infrastructure such as the power grid or Internet, using resources to hit military-specific targets such as weapons systems or R&D programs, or stealing classified or top-secret information. Beyond offensive techniques, our nation needs cybersecurity experts to defend against other nations and make sure that critical functions proceed unhindered.

The Challenge

During a conflict, it's expected that both sides will employ offensive cyberwar measures to make it harder for their opponents' commands and messages to be received on the battlefield or for critical offensive and defensive systems to function. Commands and information that aren't received in a timely manner can lead to a breakdown of strategy and planning.

Cyber operations require a strong, secure infrastructure, and a network that is unable to avoid or repel attacks is an immediate disadvantage. But a conventional routed network, even when engineered for reliability and security, may not be enough when it comes to the future of warfare.

A mission-first network is designed, implemented, and operated to adapt to the worst-case scenario. Commanders can modify network behavior as needed to ensure freedom of maneuver and freedom of action. A drone strike, a missile launch, or communicating intelligence from the field depends on a mission-first network.

A mission-first network is in sharp contrast to how conventional networks support net-ready combat and mission operations. Today, network teams are all too familiar with the painstaking, time-consuming work of modifying the network for each operation. Detailed information about IP addresses, access control lists, ports, and protocols must be at their fingertips. Planning and making the necessary changes can take weeks or months, and network teams know that as more network reconfigurations are required to achieve a designed outcome, the more likely they will create a network that is brittle and prone to failure.

The Juniper Networks Mission-First Network Solution

The Juniper Networks mission-first network transforms the traditional ways of adapting the network to mission operations. The result is a self-driving, intent-based network that is ready for net-enabled combat and mission requirements.

The foundation is the Juniper® Session Smart™ Router, which creates an advanced, service-centric network fabric that extends from client to cloud. Together, the Session Smart Router and Juniper Session Smart Conductor create the agile, secure, and resilient WAN connectivity that's required for command and control, intelligence, surveillance and reconnaissance (C2ISR)—and with greater simplicity and operational efficiency than ever before.

In a conventional routed network, packets are routed at Layer 3 OSI in a stateless fashion, which adds complexity and creates the requirement for tunnel-based transport to create capabilities like SD-WAN.

The Session Smart Router is a new type of router which routes sessions at Layer 4+, rather than individual packets at Layer 3. Unlike a legacy SD-WAN approach, it does not use overlay tunnels and adds zero overhead. The Session Smart Router transcends the inherent brittle architecture and uses network resources more efficiently than traditional routers.

The Session Smart Router's tunnel-free architecture enables up to 75% reduction in headend infrastructure costs and a 15% to 50% reduction in bandwidth usage[1], which is especially critical when conducting operations with degraded connectivity and limited bandwidth.

Features and Benefits

A mission-first network is smart.

The Session Smart Router realizes the vision of intent-based networking. It is able to achieve this vision because it's a "new" type of router.

With the Session Smart Router, the intent of mission planners and the data model used to configure the network and the desired outcomes are aligned as closely as possible, enabling a new level of agility and control. The time-consuming, painstaking gap between the planner's intention and the network configuration is closed—all because sessions are routed statefully across the fabric with end-to-end context, rather than routing packets as with a conventional routed network.

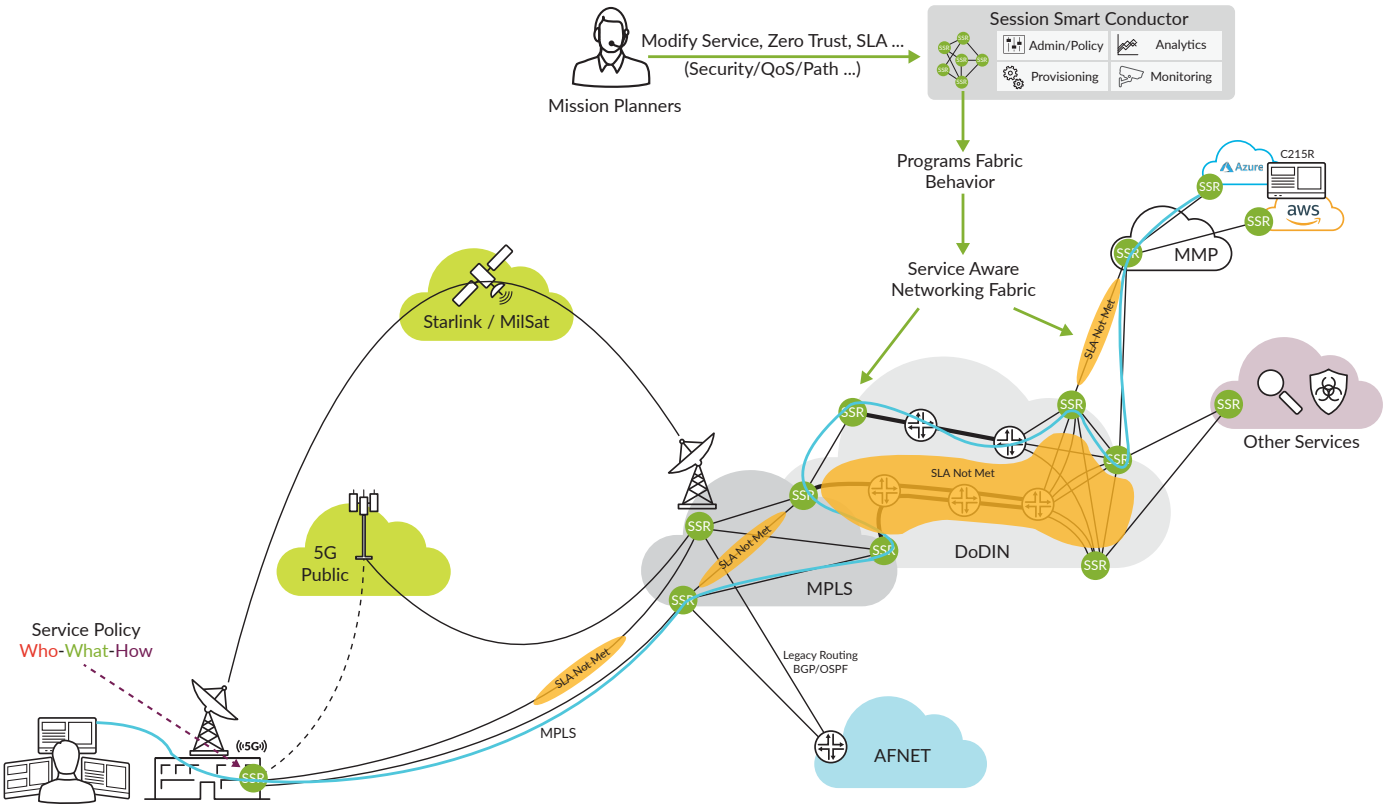

Figure 1: Juniper Session Smart Router creates an advanced, service-centric network fabric, delivering agile, secure, and resilient WAN connectivity required for net-enabled combat and mission operations.

[1] A 15% to 50% reduction in bandwidth usage is based on packet size when compared to legacy tunnel based approaches.

The Session Smart Router enables the creation of a simple, reliable, application-aware network fabric that meets the most stringent performance, availability, and security requirements. Two unique control planes—the service-centric control plane and the session-aware data plane—create an intent-based network that can be rapidly adapted to changing mission requirements and environments.

During cyber operations, leaders need to ensure freedom of maneuver[2] and freedom of action while denying the enemy the same. If cyber operations require immediate maneuvering in cyberspace or changing network posture or behavior programmatically, the Session Smart Router makes it easy by routing sessions.

The Session Smart Router puts every session into context by asking three fundamental questions:

- Who is the source of the traffic?
- What is the intended destination?
- How should the network behave?

If the "who" is allowed access to the "what," then the Session Smart Router determines "how" the session should be escorted to its destination in the most optimal way, based on the mission planner's intent and the current state of the network. Global policy definitions ensure consistency everywhere, and policies can be updated in just a few mouse clicks.

With tight alignment between the mission intent and network data model, the Session Smart Router understands how each session is related to a user, device, or application, its intended destination, and if policy allows, how the traffic should be escorted across the network. Policies are applied per session, not per tunnel, as with legacy SD-WAN solutions. Traffic can be delivered across any type of IP connectivity, such as 5G, LTE, SATCOM, MPLS, mesh networks, or public Internet.

The result is a network that's intelligent, adaptable, resilient, and secure. The Session Smart Router operates even when disconnected from orchestration, giving remote operators the ability to modify network behavior, view analytics, and modify configuration with the same local user interface and APIs. This allows for full functionality even in denied, degraded, intermittent, or limited (DDIL) environments.

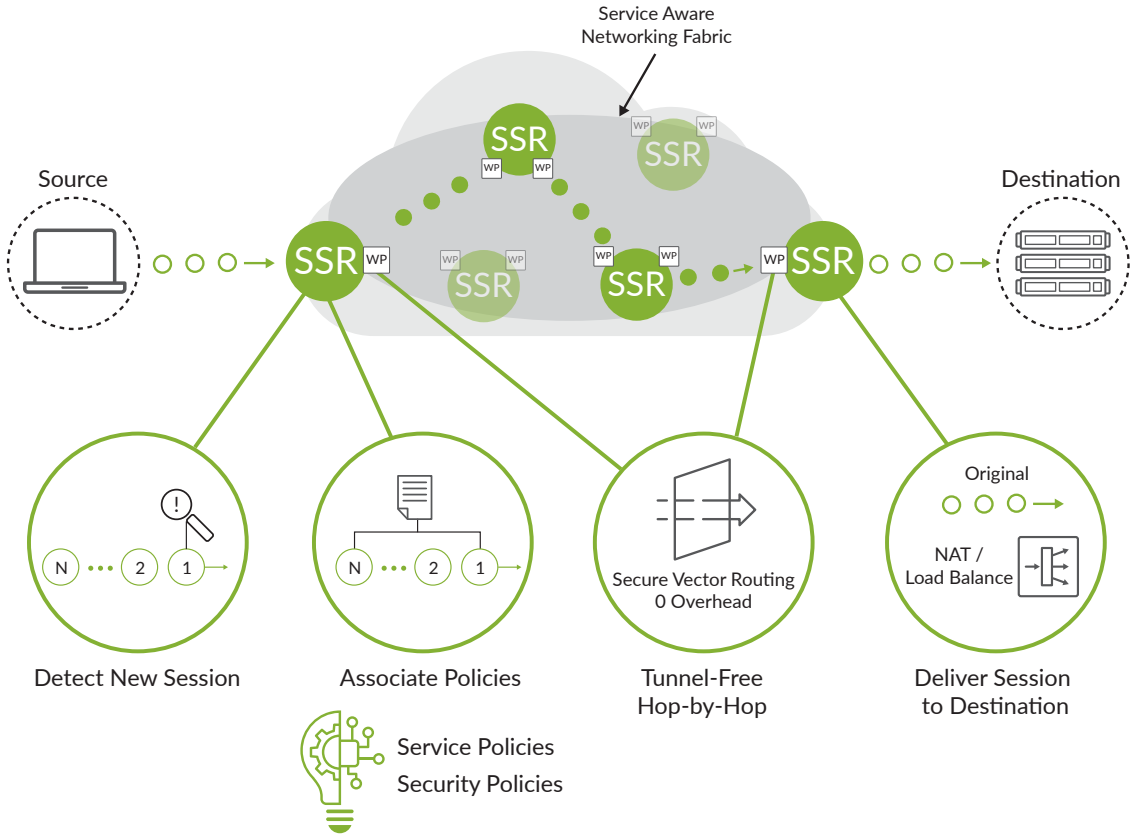

Figure 2: With a Juniper mission-first network, planners can align their mission intent and network data model, resulting in a network that can be changed quickly, easily, and with little advanced notice.

[2] Department of Defense, Joint Chiefs of Staff. " Joint Publication 3-12 - Cyberspace Operations." JP 3-12, Joint Chiefs of Staff, 8 June 2018, www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf?ver=2018-07-16-134954-150. Chapter 2. 5. e. "Movement and Maneuver"

A mission-first network is resilient.

With the Session Smart Router, leaders gain situational awareness over the network, with clear visibility into the state of the network, each session's performance, the location of the users, and how critical workloads are performing, all in real time, helping to create a common operational picture[3]. With this awareness, mission planners can make quick adjustments to the network behavior to ensure the desired outcomes, ensuring reliable application delivery even during rapidly changing network conditions.

The Session Smart Router uses separate management, data, and control planes to enable a more resilient network. A Juniper mission-first network can operate in DDIL bandwidth environments—all while providing local operators the same user interface and analytics capabilities on each router, ensuring operators can maintain freedom of maneuver at all times.

Fine-grained session-based analytics and reporting deliver maximum visibility into how applications and the network itself are performing. Application and network performance analytics are available via the GUI and RESTful APIs, and IPFix-based session detail records are generated on a per-session basis and stitchable across NAT boundaries using globally unique Session-ID assigned to each session.

In the midst of cyber operations, a desired network path may become damaged or go offline. The Session Smart Router can intelligently route traffic from one user to an application while maximizing available bandwidth as no legacy tunnels are used. The Session Smart Router can even limit or temporally disable non-mission-critical traffic during periods of degraded connectivity. In addition new points of presence for network access can be created as needed—changing the network terrain. If issues exist the network will self-remediate or provide pinpoint accuracy as to the location of the fault.

A cyber battlefield is defined based on where you are, thus obfuscating critical communications between endpoints can make it more difficult for adversaries. The Session Smart Router enables the obscuring of network behavior by eliminating IPSec-based encapsulation (which is easy to spot), and by utilizing the Session Smart Routing for Classified (SSRfC) architecture to create mission-specific networks that may only exist for days or even hours.

A mission-first network is secure.

It's critical that a network constructed for cyberwarfare is able to avoid or repel attacks and allow freedom of maneuver. With Juniper Connected Security, security is embedded into the network fabric itself, creating a Zero Trust network.

The Session Smart Router provides native firewall, intrusion detection and prevention (IDP), traffic engineering distributed denial of service (DDoS) management, and access control, which can be tailored at the individual session level. Global policy definitions allow for consistent security and hyper-segmentation across networks, eliminating the need for context-specific firewall filters. FIPS 140 encryption can be applied by policy to provide end-to-end data protection with no decryption on middle-hops.

User and device access to data, applications, and other resources is tightly controlled and monitored. A Juniper mission-first network can prevent breaches caused by privileged access abuse, because each piece of traffic must prove that it is authorized to access the network. Mission planners can easily define who is allowed to access applications and services, then deploy that policy globally and modify it on demand to define where, when, and to whom an encrypted data session will be allowed.

Additionally, telemetry data from the Session Smart Router can be exported to Splunk, Elastic, or Juniper Healthbot. Those tools can apply machine learning to identify anomalous behavior and use that intelligence to automatically change how traffic is routed when a threat is identified.

Solution Components

The solution is comprised of two primary components: Session Smart Router and Session Smart Conductor. Together, they form a single logical control plane that is highly distributed, and a data plane that is truly session-aware.

The Session Smart Router combines a service-centric control plane and a session-aware data plane to offer session routing, policy management, end-to-end visibility, and performance analytics. As a software-only solution, the Session Smart Router supports deployment flexibility and full high-availability.

The Session Smart Conductor is a centralized management and policy engine that provides orchestration, administration, zero-touch provisioning, monitoring, and analytics for the distributed Session Smart Router—while maintaining a network-wide, multitenant service and policy data model.

[3] Department of Defense, Joint Chiefs of Staff. " Joint Publication 3-12 - Cyberspace Operations." JP 3-12, Joint Chiefs of Staff, 8 June 2018, www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf?ver=2018-07-16-134954-150. Chapter 4. 2. d 4. "Situational Awareness"

At the heart of the Session Smart Router platform is Secure Vector Routing (SVR). SVR is a transformational new routing architecture that enables the network to differentiate the way it delivers applications and services. SVR replaces tunnel-based network overlays and inefficient provisioning systems with distributed control, simple intelligent service-based routing, and in-band (data plane) session-based signaling.

SVR is fully compatible and interoperable with existing network architectures, and Session Smart Router has full support for OSPF, BGP, VRF, etc. This allows Session Smart Router to be gradually introduced into an existing IP network without affecting the network endpoints or hosts.

The Session Smart Router can be placed at strategic locations to support mission operations and increase network visibility. As a software solution, Session Smart Router can be deployed in any physical or virtual environment, including on white-box customer premises equipment (CPE), data center network servers, or as a container in the cloud—all while being completely air-gapped. And, as a software only, on-premises solution, Session Smart Router does not require FedRAMP authorization, accelerating deployment time. Lastly, the flexible license model significantly reduces the overall compared to legacy routing or SD-WAN solutions.

A Juniper mission-first network integrates smoothly into a service-oriented IT workflow. The Session Smart Router can be configured to integrate with ServiceNow, Remedy, or a similar IT service management platform. IT operators can define service levels and policy for a particular mission, and the network behavior can be adapted while following stringent change control management processes. There's no more waiting for the network engineering team to make manual changes.

Summary—The Future is Unpredictable. Be Ready for Anything

It is impossible to accurately predict what the future of cyberwarfare will look like. That's why it pays to be prepared for all eventualities.

With a Juniper mission-first network, you have a strong foundation for command and control, intelligence, and surveillance operations. Mission planners have tight control over how the network behaves under both optimal and nonoptimal conditions. And when disruptions occur, either because of an adversary or unforeseen event, the network is resilient in real time, safeguarding the communications that support a successful outcome.

Next Steps

Juniper has extensive experience working with federal agencies and supporting their specialized network and security requirements. We offer IC/DoD-certified solutions for those missions that demand unfailing network performance.

Read the whitepaper, Session Smart Routing: How It Works.

Learn more about Juniper solutions for Federal.

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.

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

Juniper Networks - Federal
2251 Corporate Park Drive
#100
Herndon, VA 20171 USA
Phone: +1.408.745.8912
www.juniper.net/federal

JUNIPER NETWORKS | Driven by Experience™