JUNIPER NETWORKS | Federal

SESSION SMART ROUTING FOR CLASSIFIED NETWORKS

A revolutionary way to provide end-to-end control for air-gapped mission-first networks using secure vector routing.

Challenge

Federal departments and agencies need mission-first networks to support classified and unclassified traffic on the same infrastructure without losing performance and agility, all while maintaining security and air-gap requirements.

Solution

The Juniper Session Smart Routing for Classified (SSRfC) solution delivers security and agility at the highest levels. The solution combines secure vector routing with domain-specific features of the Session Smart Routing to create a secure routing architecture, providing agility and visibility in NSA High Assurance Internet Protocol Encryptor (HAIPE) Type 1 or Commercial Solutions for Classified (CSfC)-based networks.

Benefits

- *Control black-side network behavior from the red side*
- *Save 50% or more on bandwidth vs. tunnel-based approaches*
- *Gain visibility into black-side transport availability and performance*
- *Take advantage of mission-aware routing, QoS, encryption, and diverse transports*

Solution Brief

The Challenge

Federal networks that need to secure sensitive and classified data in-flight leverage NSA High Assurance Internet Protocol Encryption (HAIPE) or Commercial Solutions for Classified (CSfC)-based architectures. In these architectures, the networks have multiple layers. The outer layer becomes a black/grey transport with a red network inside. While these networks meet the security requirements customers demand, they lack the visibility and agility necessary for the cyber battlefield. The ability to see, control, and adapt these networks while maintaining the air-gap is critical.

The Juniper Session Smart Routing for Classified Solution

The Juniper® Session Smart™ Routing for Classified (SSRfC) solution provides cyber operators with the movement and maneuverability required to ensure that mission operations and other critical functions proceed unhindered even under adverse conditions.

The SSRfC architecture combines secure vector routing with domain-specific features of the Session Smart Routing to create a double-bookended secure routing architecture that provides HAIPE- or CSfC-secured networks with greater control and visibility than previous approaches (see Figure 1). SSRfC allows mission planners to execute quickly mass and maneuver in cyberspace.

Secure vector routing (SVR), currently an IETF RFC draft, is a transformational new routing architecture that enables the network to deliver applications and services in a session-aware manner.

Secure vector routing provides a completely tunnel-free transport mechanism that routes sessions instead of each packet. SVR is a departure from the traditional approach of using an overlay network of tunnels to create virtual networks and is fully compatible and interoperable with existing network architectures.

The Juniper SSRfC architecture allows cyber operators to:

- Save 50% or more on bandwidth vs. tunnel-based approaches
- Control black-side network behavior from the red side
- Observe black-side transport availability and performance from the red side
- Operate completely disconnected from other networks and orchestration

The SSRfC approach ensures that the mission intent and the network data model provided by secure vector routing are tightly aligned. The data model provides a clear understanding of 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.

With SSRfC, the network is simpler to secure and manage. Route tables are not simply a bunch of indecipherable subnets and next-hops but named entities in the data model. Network operators can modify network behavior based on specific users or applications with just two clicks. Unlike legacy approaches, there are no complex access control lists to manage and maintain for quality of service (QoS), routing, and security.

In addition, the absence of tunneling overhead saves 50% on bandwidth vs. tunnel-based approaches and delivers an optimized user experience. With SSRfC, federal organizations can maximize resource efficiency at all times.

SSRfC is also a transport-agnostic solution, allowing traffic to be delivered across any type of IP connectivity, such as 5G, LTE, Satcom, MPLS, mesh networks, or the public Internet, to support highly resilient communications.

Features and Benefits

Provide Mission-Aware Routing

The Session Smart Routing solution routes at the session layer and not the packet layer. Juniper developed a domain-specific feature for the SSRfC solution called DiffServ code point (DSCP) steering, which allows the Session Smart Routing solution to split a single IPsec session by the DSCP value. The Session Smart Router can create 64 different logical sessions from a single IPsec session, where each session maps to a specific service. Each service can have its own policy for how traffic is routed, secured, QoS applied, and assured for delivery in the Session Smart Routing data model.

See Through the Air Gap

The Session Smart Routing solution leverages the secure vector routing concept of neighborhoods which allows peering adjacencies to be established over different types of transport. These peering adjacencies can utilize DSCP values to influence how peering-related traffic traverses the network. SSRfC provides operators on the red-side network with the ability to see the state of black-side transport (see Figure 1).

Create Secure Networks from End to End with Dynamic Multihop Routing

Session Smart Routing provides mission planners with a simple and easy to administer intelligent multihop routing architecture. Whereas tunnel-based approaches are overly complex, secure vector routing enables federal IT teams to create secure, multihop networks easily. The approach is so easy that many Juniper customers deploy Session Smart Routers down to the distribution layer, which is very difficult with legacy SD-WAN technologies.

Enhance Mission Agility with Session Routing

Secure vector routing allows mission planners to set path options using vectors and network state. Different orders and weights may be assigned to different vectors, and vectors can be excluded for specific applications. Vector priority, lowest latency, or highest mean opinion score (MOS) can be used to choose paths to support different applications and service levels. Paths can be excluded or moved based on an SLA violation. Sessions can be protected with packet duplication, duplication, and adaptive forward error correction (FEC) capabilities.

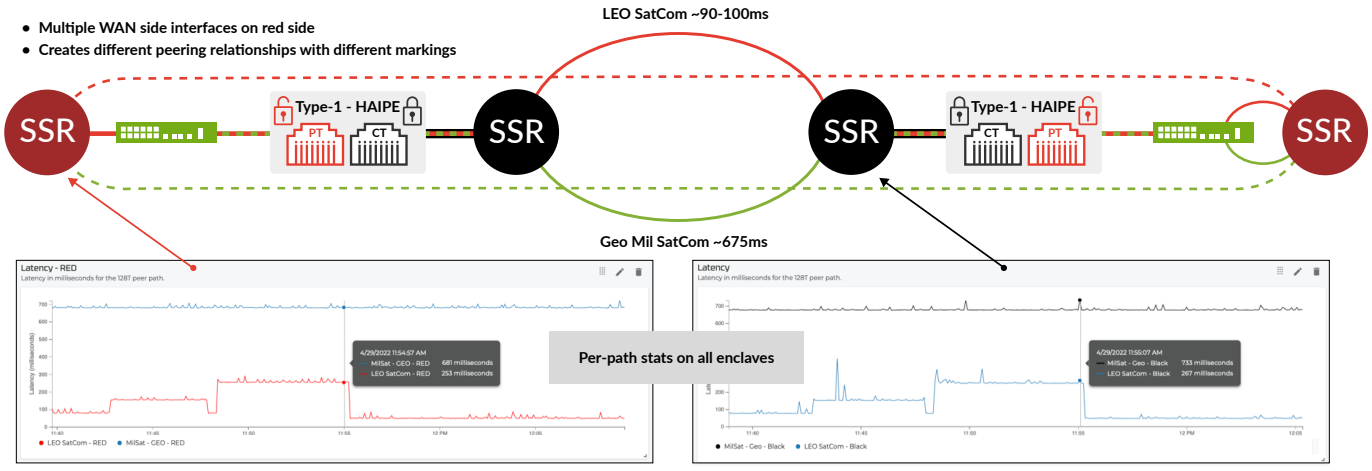

Figure 1: The Juniper SSRfC solution allows operators on the red-side network to see through the air gap to the state of the black-side transport.

Figure 2: Mission planners can create a double-bookended network with secure vector routing. The SSRfC architecture combines secure vector routing with domain-specific features of the Juniper Session Smart Router to create a double-bookended secure routing architecture that provides IPsec-based encryptors (HAIPE or CSfC) with greater visibility and control than previous approaches.

Strengthen IPsec with Protected Key Exchange

Juniper Session Smart Routing can enhance the security and resiliency of IPsec. Session Smart Routing can be configured to ensure that the key exchange only traverses trusted paths. Alternatively, Session Smart Routing can be configured to utilize packet duplication or FEC to provide message assurance to the IPsec Key Exchange process.

Enforce Service Levels Per Session with Stateful Quality of Service

The stateful QoS capabilities of the Session Smart Routing solution allow mission planners to determine service levels per session and globally. The bandwidth available for both upload and download can be controlled per session and service or for a group of services, ensuring operational resilience during mission-critical communications or actions.

Support Message Assurance for DDIL Operation

Session Smart Routing supports message assurance for Denied, Disrupted, Intermittent, and Limited (DDIL) operation, in which sessions leverage packet duplication to duplicate packets across all available paths to ensure message delivery. When lossy paths are detected, adaptive forward error correction can also be applied to decrease the probability of packet loss—message assurance functions in conjunction with packet duplication. Further, in jamming scenarios, Session Smart Routing can detect the outcome of such events and stop or limit noncritical traffic.

Set and Enforce Encryption Policies

Mission leaders can set security policies for each service or multiple services. With the SSRfC solution, network administrators can define policies governing encryption algorithms and keys. Adaptive encryption can be used to automatically not encrypt traffic that's already encrypted, such as with Transport Layer Security (TLS) or Encapsulating Security Protocol (ESP). Peer- and path-based encryption allows you to add encryption selectively, such as if you only want to encrypt when going across commercial transport.

Putting It All Together: How SSRfC Works

Let's take a look at how SSRfC works to provide mission-aware routing (see Figure 3).

Red Side

1. A user initiates a session towards a destination which enters the Session Smart Routing fabric.
2. The Session Smart Router then classifies the source tenant and destination service. The service identified uses a specific service policy which will cause the traffic to be marked on egress.
3. Traffic egresses the Session Smart Router with the specified DSCP value.

HAIPE or CSfC

4. The black Session Smart Router receives a session from the HAIPE CT interface IP destined to another HAIPE CT interface on the far side of the HAIPE device. This packet is evaluated the same way in Step 1. An additional action is performed on the Session Smart Router receiving interface to evaluate any DSCP marking applied to the packet. This marking is used to further identify the specific service (up to 64) associated with the relationship between the two HAIPE encrypters.

Black SSR

5. The black Session Smart Router makes the relevant routing and QoS decisions based on the service's assigned policy. The context for the tenant and session identified in Step 4 is embedded into the payload portion of the packet. Payload encryption and packet HMAC are also applied based on the security policy associated with the service. Markings between the black Session Smart Routers can safely be stripped without impacting metadata context.
6. When the far-side Session Smart Router receives traffic (see right side of figure), the metadata is extracted, and traffic is decrypted. Markings can be reapplied on egress from the Session Smart Router, and the encryptor can process packets in the reverse of Step 3.

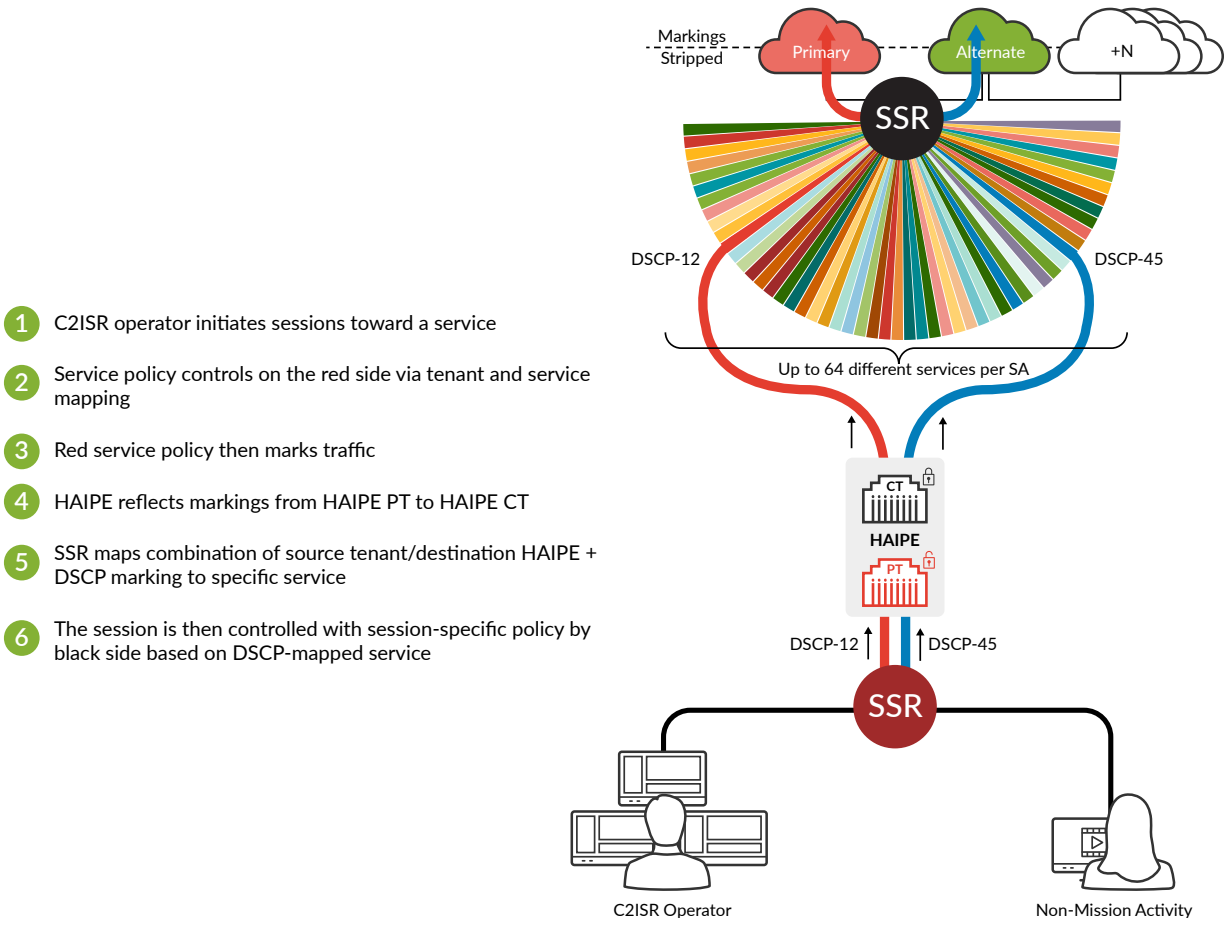

Figure 3: A look at how the SSRfC solution works to initiate and control sessions.

After step 6, the Session Smart Router will use encrypted metadata to communicate context between other Session Smart Routers. If Network Address Translation (NAT) occurs or DSCP values are stripped or re-marked in flight, it will not impact the solution.

To provide unprecedented agility, one simply needs to define the services on the black side. Mission planners can modify service policy settings on the red side, which influence markings, and then control how black-side transport is utilized.

Let's take a look at how the SSRfC solution works from end to end:

1. Looking at the left side of Figure 4, sessions are processed by the Session Smart Router on the red side using the secure vector routing data model. Specifically, the Session Smart Router evaluates who is the source of the traffic and if the user and device are authorized to access what they are attempting to access. Session Smart Router then assigns a service policy to the session based on the identified service.
2. Authorized sessions then leverage the associated service policy to control routing and QoS. This includes the ability to control path selection on the red side and how traffic entering the HAIPE/CSfC network is marked. The context for the tenant and session identified in Step 1, known as metadata, is embedded in the payload portion of the packet. Markings are applied to each packet for the session. Payload encryption and packet keyed Hashed Message Authentication Code (HMAC) are also applied based on the security policy associated with the service.
3. The HAIPE then reflects the markings sent to the plain-text interface on associated packets exiting the cipher-text interfaces.
4. The black Session Smart Router receives a session from the HAIPE CT interface IP destined to another HAIPE CT interface on the far side of the HAIPE device. This packet is evaluated the same way as in Step 1. Additional action is performed on the Session Smart Router receiving interface to evaluate any DSCP marking applied to the packet. This marking is used to indentify further the specific service (up to 64) associated with the relationship between the two HAIPE encryptors.

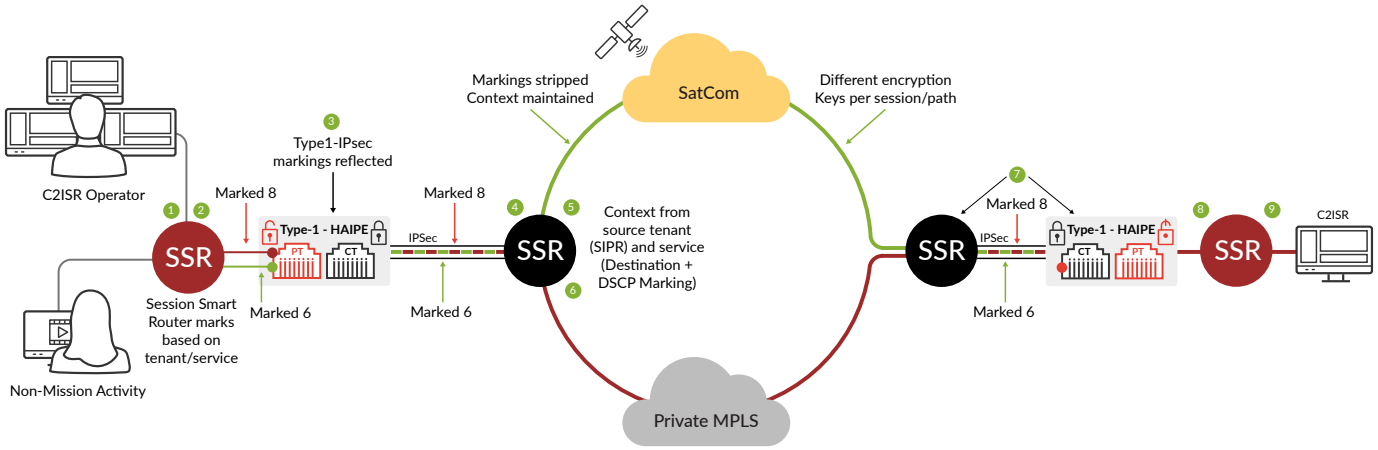

Figure 4: How the SSRfC solution works from end to end.

5. The black Session Smart Router makes the relevant routing and QoS decisions based on the service's assigned policy. Markings between the black Session Smart Routers can safely be stripped without impacting metadata context.
6. The context for the tenant and session identified in Step 4 is embedded into the payload portion of the packet. Payload encryption and packet HMAC are also applied based on the security policy associated with the service.
7. When the far-side Session Smart Router receives traffic (see right side of figure), the metadata is extracted, and traffic is decrypted. Markings can be reapplied on egress from the Session Smart Router, and the encryptor can process packets in the reverse of Step 3.
8. The red Session Smart Router receives the metadata and uses it to understand the context of the session and how it should be delivered toward the destination. Now we have established a session on both red and black sides with full context through the air gap.
9. Subsequent packets processed by the Session Smart Router will be marked as they are sent to the HAIPE encryptor, allowing for proper traffic steering and network symmetry. The marking requirement is conveyed via metadata, guarnteeing symmetric marking.
10. Should network conditions change, the Session Smart Router will process sessions the same way, providing a genuinely resilient network in DDIL bandwidth environments with zero overhead.

Solution Components

The Juniper SSRfC solution consists of the Session Smart Routing, with additional capabilities, and Juniper® Session Smart Conductor™ deployed in each enclave. Software-based Session Smart Routing can be deployed bare metal, virtual or in the cloud. The entire solution can be deployed 100% on-premises and fully air-gapped.

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

Additionally, Juniper federal services are designed to provide an enhanced, secure, end-to-end U.S.-based customer support experience, including Advanced Care Service, Advanced Care Plus Service, Premium Care Service, Flexible Services Credit, and High Security Return Materials Authorization and Non-Return Service.

Summary—Performance, Agility, and Security to Enable Multiple Classification Levels

The Juniper Session Smart Routing for Classified (SSRfC) solution delivers security and agility at the highest levels. With this solution, federal agencies can support multiple classification levels with the same infrastructure, using mission-aware routing, QoS, encryption, and diverse transports. Leveraging an SSRfC solution allows agencies to control black side network behavior from the red side and maintain traffic symmetry to rapidly and securely deliver on missions that protect national security.

To learn more, read the whitepaper Session Smart Routing: How It Works.

Read the IETF Secure Vector Routing draft RFC.

Interoperability

Juniper is CSfC provider of technology for the US federal government. See Juniper's CSfC approved solutions.

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.

To learn more about Juniper solutions for federal, visit www.juniper.net/us/en/solutions/federal-government.html.

Contact your Juniper Federal Services team at federal-services@juniper.net or call us at the federal contact support at 833-900-1454.

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

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

Copyright 2023 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property 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.

3510732-002-EN May 2023