JUNIPer SSR120 Session Smart Router User Guide

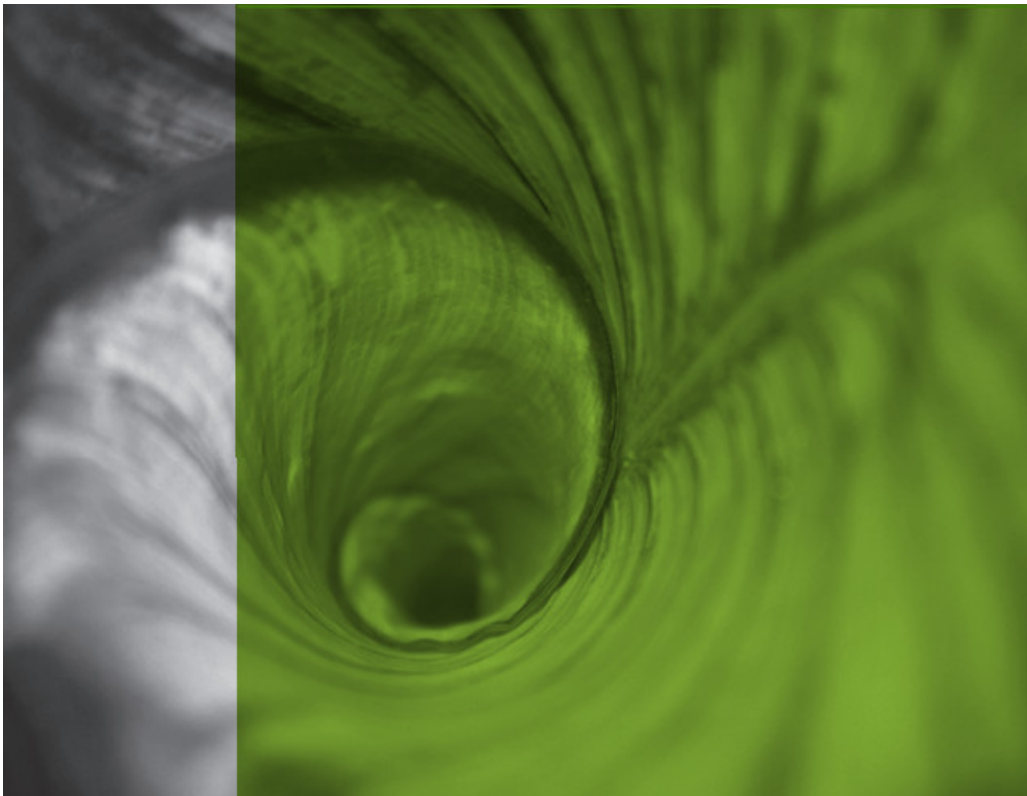**AI-DRIVEN SD-WAN:**
BUILDING NETWORKS WITH
SECURITY AT THEIR CORE

Protect infrastructure, intellectual property, and confidential information with the innovative Session Smart ™ Router (SSR)

Challenge

Despite myriad defense strategies, cyberattacks continue to proliferate. Traditional security techniques aren't enough to protect today's network, and this puts enterprises at risk.

Solution

The AI-driven SD-WAN solution, powered by the Session Smart Router (SSR), provides native Zero Trust Security, leverages hypersegmentation, and integrates multiple middlebox functionalities on a single platform. This simplifies network architecture, protects information assets, and minimizes costs.

Benefits

- ICSA corporate firewall and PCI certification

- Layer 3/Layer 4 DOS/DDOS

- Traffic engineering and URL filtering support

- FIPS 140-2 compliant

- AES256 encryption and HMAC-SHA256 per packet authentication

Cyberattacks continue to increase in size and frequency. Traditional security techniques aren't enough to protect the network, and this puts intellectual property and confidential information at risk. The innovative Juniper ® AI-driven SD-WAN solution weaves routing and network security together into one platform. With security in its DNA, every aspect of this solution was purpose-built to protect the information, applications, and services that cross the network and ultimately fuel the business.
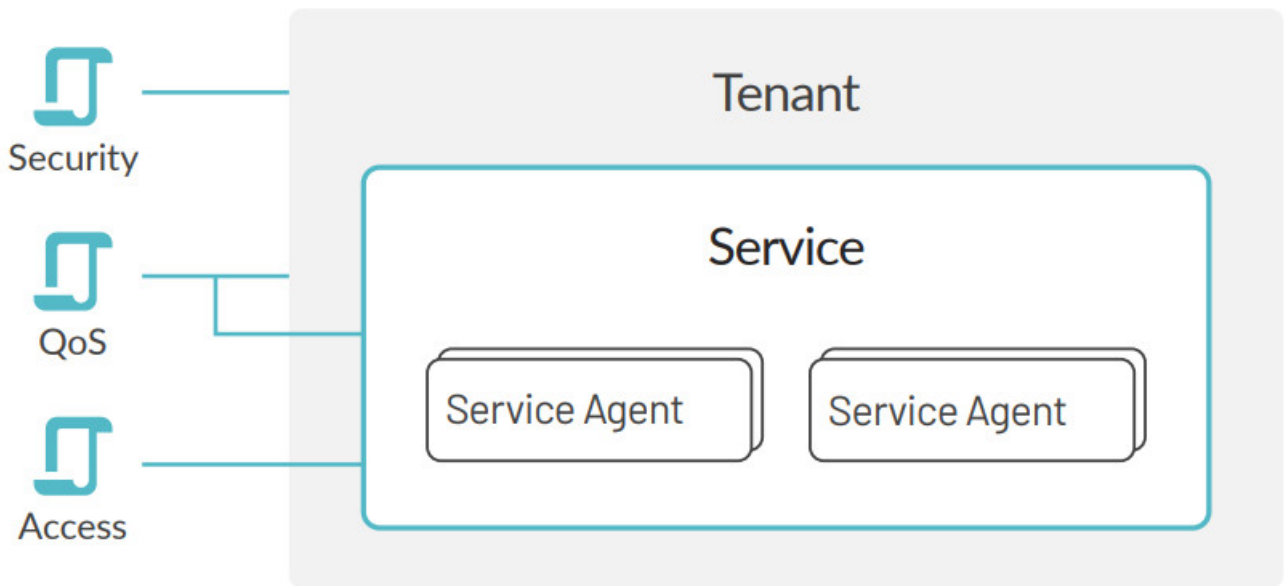
Contents

The Challenge

Despite the proliferation of various techniques to secure, restrict, or segment the network, the number of security breaches, denial-of-service (DoS) events, and other cyberattacks continues to rise. Cybersecurity Ventures predicts that cybercrime costs will reach $10.5 trillion USD annually by 2025 [1] . With built-in security that spans the entire network fabric, the Juniper AI-driven SD-WAN solution was specifically designed to reduce the exposure of networked traffic to this growing threat.

The Juniper AI-driven SD-WAN Solution

The AI-driven SD-WAN Solution combines a service-centric control plane, and a session-aware data plane to offer IP routing, feature-rich policy management, improved visibility, and proactive analytics. Unlike solutions that graft security onto an insecure network, the Juniper approach embraces the Forrester and NIST Zero Trust Model. The advanced design of the Session Smart Router (SSR) replaces the traditional routing plane with one built from the ground up with security principles at its core.

Service-Centric, Tenant-Based Security Architecture

The Juniper SSR understands sessions—dedicated links between services on the network, and the applications and users that rely on them—to perform vital business operations. The traffic crossing an SSR is processed, routed, and controlled in a service-centric manner. Services can be made to model a given application, reachable at a given address, set of addresses, or subnets. Access to these sessions is granted based on tenancy, which groups services together based on shared policies. As sessions are processed through the SSR, the tenant becomes an important construct for route determination, segmentation, classification, policy, and many other core routing principles.

Figure 1: Access to network services is based on Tenancy

With this added layer of intelligence, the solution provides the unique capability to assign security policy, quality-of service (QoS) parameters, and access control policies on a per-service, per-tenant basis. This capability makes it possible to have unique encryption and authentication keys, custom traffic engineering parameters, and tight access control at the individual session level. It also offers a flexible way to segment and isolates traffic, enabling administrators to apply different profiles based on the application or service that the session contains. Further fine-tuning of content access is provided through URL filtering.

Zero Trust Security

Forrester's Zero Trust Model of information security revolves around the "never trust, always verify" principle. With Zero Trust security, there is no automatic trust for any entity—including users, devices, applications, and packets —regardless of what it is and its location on, or relative to, the network. Similarly, The National Institute of Standards and Technology (NIST) SP 800-207 Publication, Zero Trust Architecture (ZTA), defines a ZTA as a network that does not implicitly trust users, assets or resources based solely on their physical or network location. In a world of on-the-go employees and on-demand services, the Zero Trust Model is intended to shrink trust zones, reduce attack surfaces, and restrict lateral movement if a resource is compromised. With inherent network virtualization and infused security functions, the AI-driven SD-WAN solution can create zero-trust security boundaries that compartmentalize different areas of the network. In doing so, businesses can protect sensitive information from unauthorized applications or users, minimize the exposure of vulnerable systems, and prevent the lateral movement of malware throughout the network.
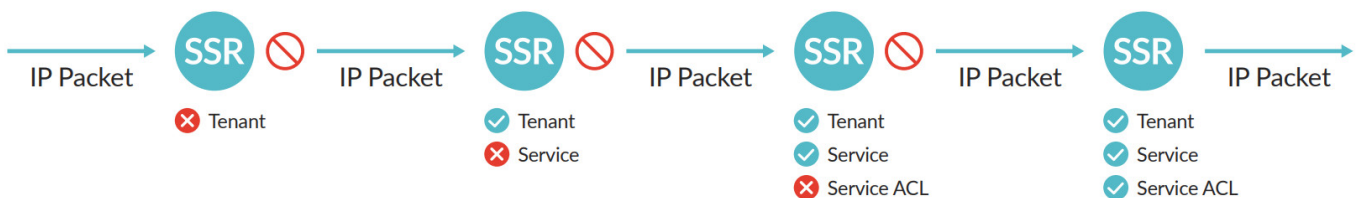
Figure 2: Deny-by-default policy

AI-Driven SD-WAN: Building Networks with Security at Their Core

Unlike a traditional SD-WAN solution, which follows an "allow-by-default" policy, the AI-driven SD-WAN solution follows the principle of "deny-by-default," which uses a series of checkpoints to validate legitimate network traffic.

- When a packet hits an SSR, the first check is to verify whether the packet belongs to a tenant.
- If the packet does not belong to a tenant, the packet will be dropped.

- When the packet belongs to a tenant, the next check is to verify whether it is destined to a service that 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.
- When the destination of the packet belongs to a service, the router examines the context-specific access control list (ACL) to determine whether the source of the packet is allowed access to the service.
- If the source is denied access to the service, the packet will be dropped
- Once the packet passes the preceding checks, the packet will be forwarded to the next hop toward the destination. Unless an enterprise explicitly allows a session to cross the network, the SSR will drop all packets belonging to a session that does not clear the series of checkpoints. While performing the series of checks for every packet, the SSR maintains the rate of traffic speed to match the line rate.

Features and Benefits

- Service-centric, tenant-based security architecture: enables the SSR to understand sessions and perform vital business operations.
- Zero trust security: The SSR follows the principle of "deny by-default," which uses a series of checkpoints to validate legitimate network traffic.
- Full network firewall functionality: ICSA-certified and PCI compliant, SSR includes advanced features such as URL filtering for the control of web page access.
- Security at its core: The advanced design of SSR replaces the traditional routing plane with one built from the ground up with security principles at its core.

Summary—Zero Trust Security at the Network Core
The AI-driven SD-WAN approach to zero trust security allows the network to be built around the services it's meant to deliver, addressing the cyber threats that target today's hyperconnected environments. With native security controls that replace obsolete perimeter-based solutions and integrated features that would otherwise require an array of middleboxes, AI-driven SD-WAN helps enterprises protect the assets that are critical to their success.

Next Steps
To find out more about the Juniper AI-driven SD-WAN solution, please contact your Juniper account representative and go to **www.juniper.net/us/en/solutions/sd-wan.html**

About Juniper Networks
Juniper Networks brings simplicity to networking with products, solutions, and services that connect the world. Through engineering innovation, we remove the constraints and omplexities of networking in the cloud era to solve the toughest challenges our customers and partners face daily. At Juniper Networks, we believe that the network is a resource for sharing knowledge and human advancement that changes the world. We are committed to imagining groundbreaking ways to deliver automated, scalable and secure networks to move at the speed of business.

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

Documents / Resources

	JUNIPer SSR120 Session Smart Router [pdf] User Guide SSR120 Session Smart Router, SSR120, Session Smart Router, Smart Router, Router

References

- **SD-WAN Solutions | Juniper Networks US**

Manuals+,