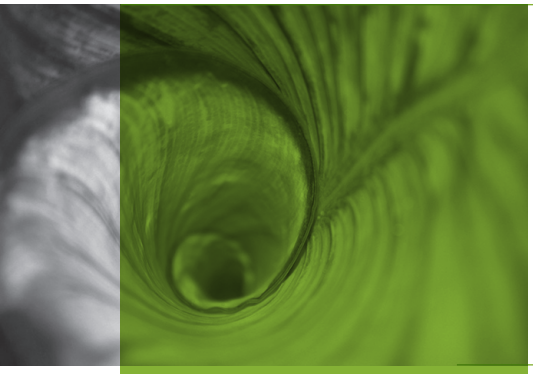

AI-DRIVEN SD-WAN: BUILDING NETWORKS WITH SECURITY AT THEIR CORE

Protect infrastructure, intellectual property, and confidential information with the Session Smart™ Router (SSR) and AI-Driven SD-WAN

Challenge

- *Cyberattacks continue to proliferate in private WANs, including SD-WANs*
- *Perimeter security techniques are insufficient to protect these networks*
- *The dominant "accept-by-default" approach often fails to validate malicious traffic*

Solution

- *AI-driven SD-WAN provides Zero Trust Security with a "deny-by-default" approach to all traffic*
- *It has built-in corporate firewall capabilities at Layers 3 and 4*
- *IDP and URL filtering are available with the Session Smart Router Advanced Security Pack*

Benefits

- *Hypersegmentation ensures that all information assets are protected from client-to-cloud*
- *Tunnel-free architecture reduces bandwidth costs by 30-50%*
- *Vital business operations are understood and performed by the SD-WAN*

Solution Brief

Cyberattacks on enterprise networks 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, powered by the Session Smart Router (SSR), weaves routing and network security together into one platform. With security in its DNA, every aspect of this solution is purpose-built to protect the information, applications, and services that cross the network and ultimately fuel the business.

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 for enterprises and service providers alike. Cybersecurity Ventures predicts that cybercrime costs will reach $10.5 trillion USD annually by 2025[1].

Prevailing techniques such as perimeter security are generally not able to stave off the worst of these attacks. Enterprises need assurances that malicious traffic doesn't get onto the network in the first place. Network wide policies do help, but seldom if ever can guarantee that unwarranted traffic will be kept off the network.

The Juniper AI-Driven SD-WAN Solution

With built-in security that spans the entire SD-WAN fabric, the Juniper AI-driven SD-WAN solution is specifically designed to reduce the exposure of networked traffic to the growing threat of attacks. The solution combines a service-centric control plane with a session-aware data plane to offer IP routing, feature-rich policy management, client to cloud visibility, and proactive analytics.

Unlike solutions that bolt security onto an intrinsically insecure network, the Juniper approach embraces the zero trust models defined by leading analysts and standards bodies such as Forrester Research and the National Institute of Standards and Technologies (NIST). 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.

[1] "Cybercrime To Cost The World $10.5 Trillion Annually By 2025," Cybersecurity Ventures Official Annual Cybercrime Report (2022).

Service-Centric Security Architecture

The Juniper Session Smart Router understands sessions—dedicated links between services and applications on the network, and the users and devices 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 the networks themselves, which groups services together based on shared policies. Sessions are processed through the SSR when they have been validated by templates that define the SD-WAN. The network is thus an important construct for route determination, segmentation, classification, and policy.

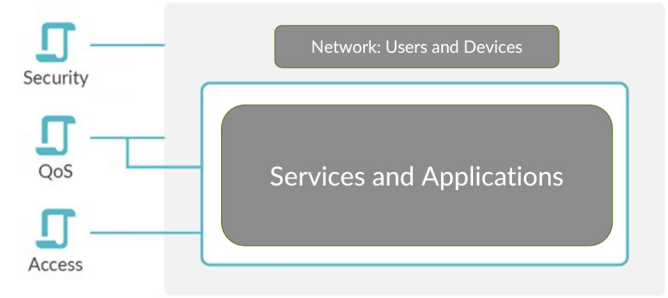

Figure 1: User and Device Access to Services and Applications is Based on Predefined Mappings in Templates

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-network basis.

The mappings shown in Figure 1 is hypersegmented into all entities that touch or affect the network, including users and their devices, network servers, WAN and LAN interfaces, application and traffic steering policies, and routing rules for the AI-Driven SD-WAN.

Further details on these techniques are available in the Guided Setup for Juniper Mist WAN Assurance, and illustrated in Implementing Branch Networks for an AI-Driven Enterprise Solution Brief.

The capabilities also include unique encryption and authentication keys, custom traffic engineering parameters, and tight access control at the individual session level. AI-Driven SD-WAN also offers a flexible way to segment and isolate 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 via an Advanced Security Pack that includes Intrusion Detection and Prevention (IDP) and URL filtering. The full set of security features in AI-Driven SD-WAN is shown in Figure 2.

This FIPS 140-2 compliant solution includes AES256 encryption and HMAC-SHA256 per packet authentication. The firewall functionality is ICSA certified and PCI compliant.

Figure 2: Security Features in AI-Driven SD-WAN

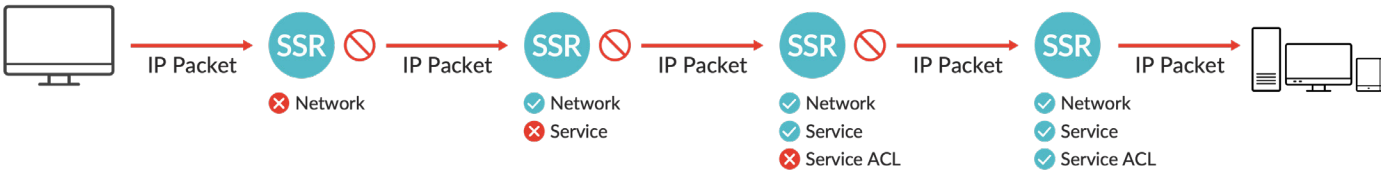

Figure 3: Deny By Default Policy

Zero Trust Security

Forrester's Zero Trust Model for 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 network as one 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.

Deny-by-Default at Every Hop

With inherent network virtualization and built-in 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.

Unlike a traditional SD-WAN solution, which follows an "allow-by-default" approach, the AI-Driven SD-WAN solution follows the principle of "deny-by-default," which uses a series of checkpoints to validate legitimate network traffic (Figure 3).

These mechanisms are provided by AI-Driven SD-WAN's Secure Vector Routing protocol and are enforced hop-by-hop and from ingress to egress:

- When a packet hits an SSR, the first check is to verify whether the packet belongs to a network
- If it does not, it will be dropped.
- Else, the next check is to verify whether it is destined to a service which the network is allowed to access.
- If the destination does not correspond to any service available on the network, the packet will be dropped.
- Else, the SSR examines a 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.

This is re-verified at every hop. Only when a packet passes all of these checks will it be forwarded to the next hop toward its destination.

Thus, 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 these checks for every packet, the SSR maintains the rate of traffic speed to match the line rate.

While competing solutions generally use tunneling technologies such as IPsec to isolate traffic, AI-Driven SD-WAN is tunnel-free, resulting in a 30-50% bandwidth savings.

Conclusion: Zero Trust Security in the SD-WAN

AI-Driven SD-WAN's 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.

AI-Driven SD-WAN is available directly to enterprises and also may be consumed through a service provider partner.

Next Steps

To find out more about the Juniper AI-Driven SD-WAN solution, please contact your Juniper account representative and go to juniper.net/sd-wan.

Resources

White Papers

Session Smart Routing—How It Works White Paper
AI-Driven SD-WAN Secures Today's Cloud-Era Networks White Paper

Video

Session Smart Router Advanced Security Pack Overview

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

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

3510706-004-EN Apr 2023