



JUNIPER MIST WAN ASSURANCE DATASHEET

Product Overview

Juniper Mist Cloud services are moving IT operations closer to the intelligent Self-Driving Network™ in the era of the AI-Native enterprise. Juniper Mist WAN Assurance delivers simpler operations, shorter mean time to repair (MTTR), and better visibility into end user experiences across the WAN.

Product Description

Juniper® Mist™ WAN Assurance is a cloud service that brings automated operations and service levels to the enterprise access layer at the WAN edge. WAN Assurance is a key component of the Juniper AI-driven SD-WAN solution, enabling IT teams to deliver superior user experiences across the WAN. When used in conjunction with [Juniper Mist Wired](#) and [Wireless Assurance](#), the service transforms and unites all operations across [network switches](#), [IoT devices](#), [access points](#), servers, printers, and other equipment. [Juniper Session Smart™ Routers](#) (SSR) and [Juniper SRX Series](#) Services Gateways provide rich streaming telemetry that enables application health, WAN link health, and gateway health metrics and anomaly detection.

The [Juniper Mist AI](#) engine and virtual network assistant further simplify troubleshooting and streamline the helpdesk with self-driving actions that automatically remediate issues. [Marvis Virtual Network Assistant](#) turns insights into actions and fundamentally transforms IT operations from reactive troubleshooting to proactive remediation.

Juniper Mist Cloud services are 100% programmable using open APIs for full automation and/or integration with your IT applications.

WAN Service-Level Experiences

Get operational visibility into user WAN experiences with service-level expectations (SLEs) for SSRs or SRX gateways. Measure the impact of both gateway and WAN circuit health on end user application experiences. A WAN Link Health SLE, which accounts for network congestion, cable issues, and ISP network availability, delivers insights into how these factors are affecting a given network user or application. The Juniper Mist SLE dashboard helps to identify root causes of suboptimal application experiences in just a few clicks to proactively isolate “needle-in-a-haystack” problems (Figure 1).

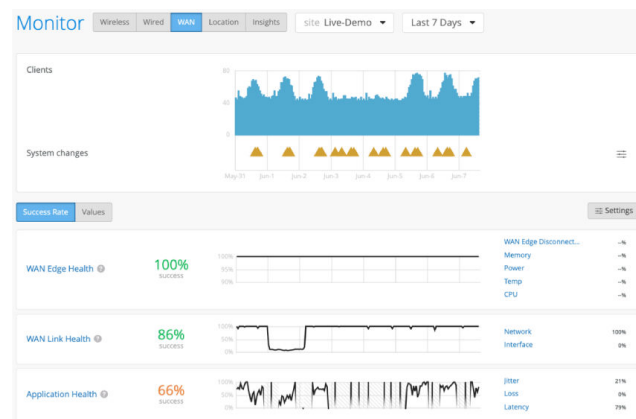


Figure 1: WAN SLEs

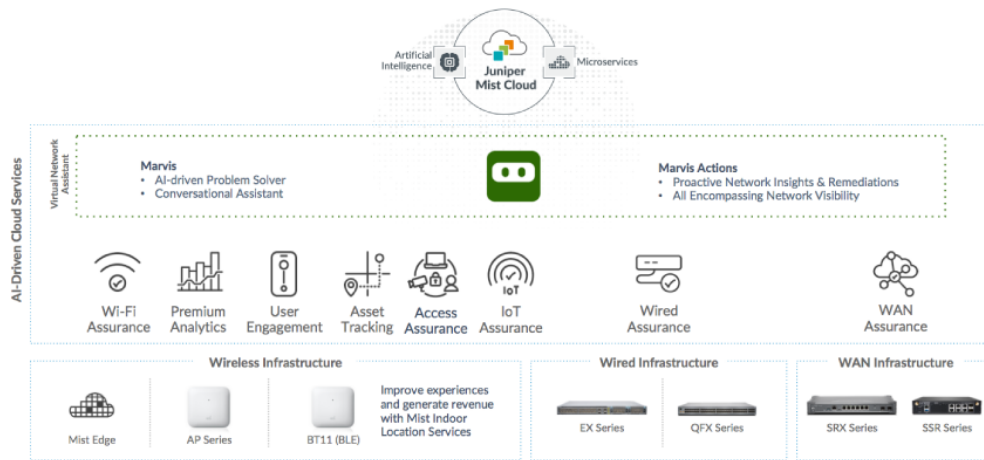


Figure 2: AI-Native Enterprise Portfolio Overview

WAN Insights Driven by Mist AI

Know exactly how SSRs or SRX gateways are performing with metrics and insights down to the port level. These include CPU, memory utilization, bytes transferred, traffic utilization, and power draw. WAN Assurance also logs gateway events, like configuration changes and system alerts. WAN and IPsec utilization insights tell you how much traffic traverses your encrypted tunnel versus your local breakout. You also get visibility into per-user and per-application performance and experiences (Figure 3).

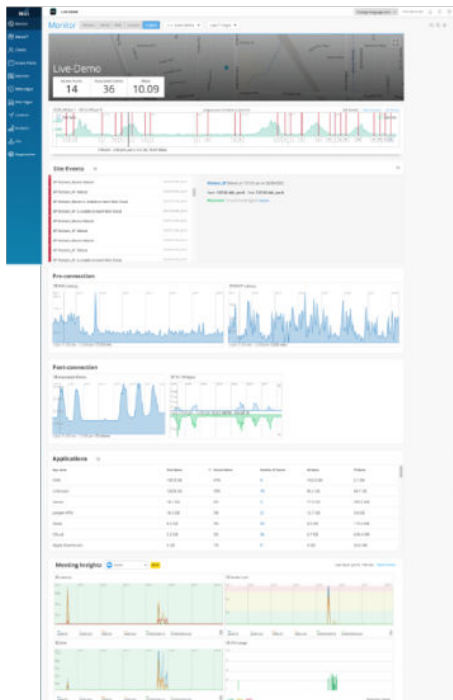


Figure 3: WAN Insights

The Congestion SLE lets operators know if their network interfaces are being overutilized and causing poor user experience. With App Routing Insights, operators can figure out what is disproportionately using bandwidth and the best way to remediate the problem. Options could be to purchase more bandwidth, adjust capacity planning, or throttle certain traffic types (Figure 4).

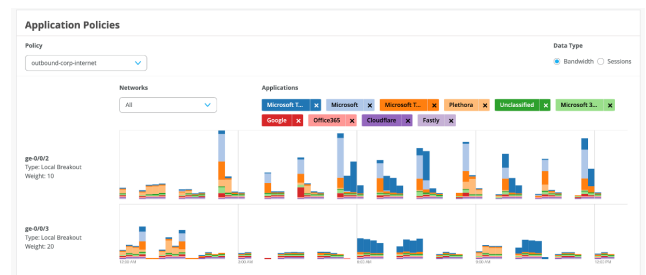


Figure 4: App Routing Insights

Dynamic packet capture (dPCAP) gives operators insights on how to shorten MTTTR and easily search for needle-in-a-haystack issues. Instead of recreating issues on the network to capture the right packets, Mist AI will notice when an issue is occurring and automatically capture the appropriate packets for analysis.

Marvis, the AI-Native Virtual Network Assistant for WAN

Marvis Virtual Network Assistant (VNA) moves IT operations closer to the Self-Driving Network with simplified troubleshooting and performance analysis for helpdesk staff and network administrators.

Marvis Actions is a one-stop information center that provides visibility into site-wide network issues that need immediate attention. Use Marvis Actions to find issues affecting user experience and get recommendations into resolutions (Figure 5).

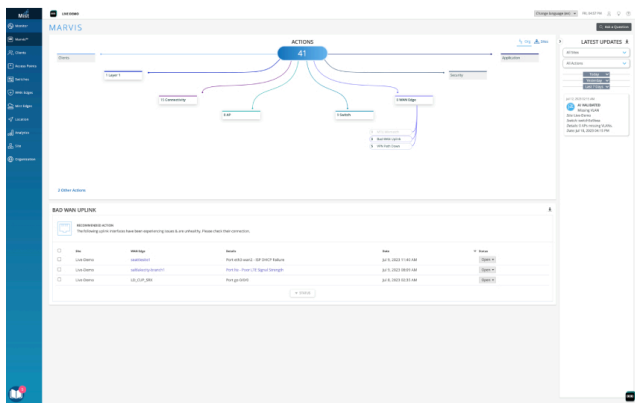


Figure 5: Marvis Actions

The Marvis Conversational Interface service allows IT teams to quickly get answers to troubleshooting questions. Simply ask a question in natural language, such as, “Why is my user’s video call experience bad?” and Marvis will provide recommendations to improve those experiences. Figure 6 shows Marvis informing IT of a WAN issue causing the CEO to have a poor video call experience.

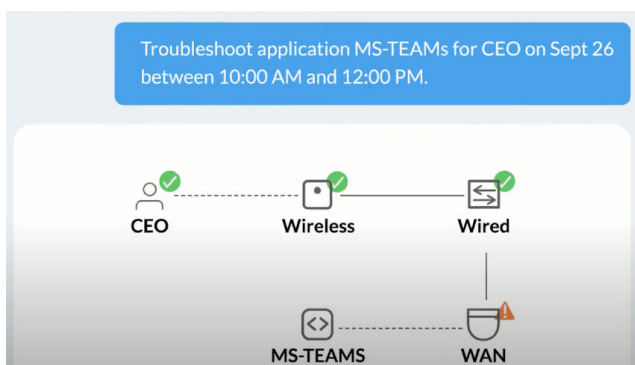


Figure 6: Troubleshooting an application

[Marvis Minis](#) perform automated speed tests that give enterprises the ability to see if they are getting the full bandwidth that they purchased. Even when users aren’t present, operators are alerted to upstream network issues. This gives operators the opportunity to work on resolving issues before end users show up to the office.

SD-WAN, Powered by Session Smart

In addition to providing [AIOps](#) for Day 2 operations, WAN Assurance delivers life cycle management and operations. This includes Day 0 and Day 1 operations for the Juniper AI-driven SD-WAN solution with Session Smart Routers that fuel an advanced, service-centric networking solution. Session Smart technology delivers an experience-based SD-WAN with deep session visibility and insights, and fine-grained session control. Its tunnel-free approach enables agile, secure, and resilient WAN connectivity with breakthrough economics and simplicity.

With WAN Assurance, IT teams can onboard, configure, and deploy SSRs and SD-WAN with operations such as:

- Zero-Touch Provisioning (ZTP) and easy onboarding with Mist Claim Code
- Easy templating for rapid scale deployments
- Path and peering preferences
- Service and application policies
- Security policies
- Network and NAT configuration

Session Smart Routers are available on dedicated appliances (Table 1).

Table 1: SSR Appliances and suggested locations

Appliance	Suggested Location	Max Throughput (Unencrypted)	Relevant Datasheet
SSR120	Small branch	1.5 Gbps	SSR100 line of routers
SSR130	Medium branch	2 Gbps (line rate on ports)	
SSR1200	Large branch or small data center / campus	10 Gbps	SSR1000 line of routers
SSR1300	Medium data center / campus	20 Gbps (max. throughput on NIC)	
SSR1400	Large data center / campus	40 Gbps	
SSR1500	Extra large data center / campus	50 Gbps (max. throughput on NIC)	

The hardware datasheets provide standard specifications such as interface options, number of interfaces, encrypted throughput, memory, and hard drive capacity.

SSRs are also available in other form factors, including certified white boxes (see the [Session Smart Routing](#) datasheet) or the Juniper® NFX Series Network Services Platforms.

WAN Assurance also supports the following [SRX Series Firewalls](#) when deployed as WAN gateways:

- [vSRX](#)
- [SRX 300](#)
- [SRX 320](#)
- [SRX 340](#)
- [SRX 345](#)
- [SRX 380](#)
- [SRX 1500](#)
- [SRX 1600](#)
- [SRX 2300](#)
- [SRX 4100](#)
- [SRX 4200](#)
- [SRX 4300](#)
- [SRX 4600](#)

Choosing a WAN Edge Device

When choosing a WAN edge platform within Juniper Mist WAN Assurance, SSRs are generally recommended for their efficiency in network utilization, quick failover, rich telemetry, and integrated security, leveraging Secure Vector Routing and AI-enhanced cloud management.

However, for networks already using Juniper's SRX gateways, integrating these with Juniper Mist enhances their capabilities and offers a more gradual transition to SD-WAN. This enables immediate AI and cloud management benefits while accommodating familiar environments.

Additionally, organizations can configure their security capabilities directly on the SSR and/or the SRX through the Juniper Mist

framework. Ultimately, the choice between SSR and SRX should align with your specific needs and goals, ensuring a seamless integration with Juniper Mist's unified management dashboard.

Advanced Security Pack

Session Smart Router's Advanced Security Pack (Figure 7) integrates further security functionality into the routing fabric:

- URL filtering prevents access to and from specific sites and to meet special business requirements
- An Intrusion Detection and Prevention System ([IDS/IPS](#)) protects against advanced malicious attacks



Figure 7: Foundational SSR router security and the Advanced Security Pack

These features eliminate the need for additional security appliances at the branch, providing this enhanced functionality within the Juniper Mist ecosystem of wired, wireless, and SD-WAN. If more cloud-integrated security is needed, customers have the option of adding [Juniper Secure Edge](#) to the environment.

Meeting You Where You Are

Juniper Networks wants to meet you where you are when it comes to your network security. The Advanced Security Pack can thus be installed standalone or alongside a Juniper [SRX Series Firewall](#) at your branch or data center.

The Advanced Security Pack can also be used to help you with your [SASE Journey](#), giving you protection in the branch or data center before easily offloading that traffic to an SSE such as [Juniper Secure Edge](#).

Risk Profiling, Driven by AI

WAN Assurance is a key component of the Risk Profiling solution that brings network security to the distributed network edge. Risk Profiling provides visibility into infected wired or wireless clients that's observable within the Juniper Mist Cloud and assigns a threat score determined by the Juniper ATP Cloud. From within the Juniper Mist Cloud, you can geospatially locate infected devices and take one-touch mitigation actions like ban or deauthenticate.

About Juniper Networks

Juniper Networks believes that connectivity is not the same as experiencing a great connection. [Juniper's AI-Native Networking Platform](#) is built from the ground up to leverage AI to deliver exceptional, highly secure, and sustainable user experiences from the edge to the data center and cloud. You can find additional information at www.juniper.net or connect with Juniper on [X](#) (formerly Twitter), [LinkedIn](#) and [Facebook](#).

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

www.juniper.net

APAC and EMEA Headquarters

Juniper Networks International B.V.
Boeing Avenue 240 1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands

Phone: +31.207.125.700

