



Optimizing Microsoft 365 with Juniper AI-driven SD-WAN

TABLE OF CONTENTS

Introduction	3
Identify and Differentiate Microsoft 365 Traffic.....	4
Connecting to the closest Microsoft 365 PoP via DIA.....	6
Customer use case	7
Summary.....	8
About Juniper Networks	8

Introduction

Juniper Networks believes that networks exist to connect users to services and applications, and network design should start with those services at the core. The [Juniper AI-driven SD-WAN solution](#) takes distributed, software-defined networking and routing to an entirely new level by speaking the language of applications, which are sessions. The solution simplifies the traditional method of routing by IP and instead applies a mindset of “routing with words” called “Session Smart” Routing. [Session Smart Routing](#) improves network simplicity and agility by eliminating tunnels and providing session awareness between endpoints. Instead of using traditional IPsec tunnels, the solution utilizes a unique protocol called Secure Vector Routing. The solution is powered by the software-defined Juniper Session Smart Router and is managed by either the Juniper Session Smart Conductor or the Juniper Mist Cloud. Together, they form a single logical control plane that is highly distributed and a data plane that is genuinely session-aware.

The Juniper AI-driven SD-WAN solution puts organizations in control of session directionality while offering fine-grained segmentation and encryption of all data in motion. It enables critical business SaaS workloads, such as Microsoft 365 that deliver mission-critical applications including Microsoft Word, Microsoft Excel, Microsoft Outlook, Microsoft SharePoint, Microsoft OneDrive, and Microsoft Teams. Microsoft has certified the Juniper AI-driven SD-WAN solution as a designated qualified networking solution that meets the requirements for “[Works with Microsoft 365](#)”. The solution enables a simple setup and a high-quality experience. Optimizing and routing Microsoft 365 traffic to the closest service endpoints with the least amount of latency results in the best end-user experience and is key to the success of workforce productivity. Juniper Session Smart Routing adheres to these key networking constructs and follows the requirements under the Microsoft 365 network connectivity principles to ensure that any Juniper Session Smart Router will efficiently and intelligently:

- Identify Microsoft 365 network traffic using Microsoft recommended endpoint API
- Allow local branch egress of Microsoft 365 network traffic to the Internet from each location where users connect to Microsoft 365
- Allow Microsoft 365 traffic to bypass proxies and packet inspection devices
- Prioritize Microsoft 365 traffic to avoid congestion

Figure 1 shows the recommended practice method for Microsoft 365 traffic to provide the optimal experience with the least amount of latency.

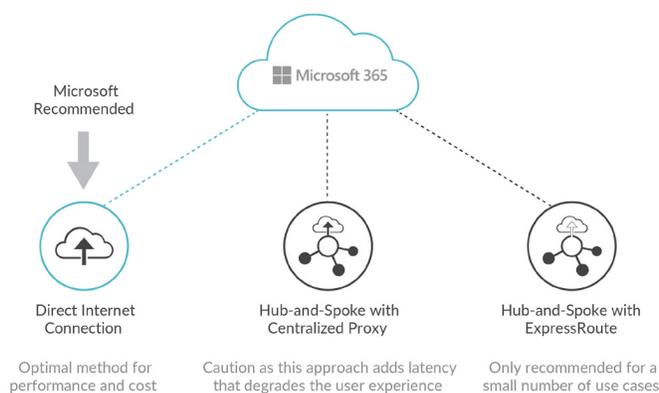


Figure 1: Microsoft 365 Recommended best practice of optimal user experience.

Whether end-users are accessing Microsoft 365 applications over ExpressRoute, over Internet and MPLS connections from the SD-Branch, and/or over Internet and wireless connections from home, Juniper Networks enables the best economic savings with reduced bandwidth and scalability to thousands of locations to route services. This seamless experience is delivered while reducing IT costs for hardware and continuous high-speed session failovers to alternate circuits in case of failures.

Identify and Differentiate Microsoft 365 Traffic

As customers migrate to Microsoft 365—there is a need to allow and provide special consideration to various workloads in the Microsoft 365 product sets, such as Teams, OneNote, Exchange Online, and so on. In an ever-changing cloud-first world, the method of IT manually whitelisting IP addresses for these SaaS services is not a scalable practice. Therefore, leveraging a published JSON file from the Microsoft 365 team simplifies the process for IT to scale out.

The Juniper AI-driven SD-WAN solution has several techniques by which it can associate traffic to named applications. This is sometimes referred to as "**Application Identification**" (or "appID"), and the feature that allows administrators to define network policies using dynamically learned content instead of static IP addresses. The Session Smart Conductor includes a Microsoft 365 application ID module that can easily be imported to apply the policies to identify the Microsoft 365 services. To classify Microsoft 365 traffic, the Session Smart Router leverages the **REST-based web service** from the Microsoft site to categorize Microsoft 365 traffic. A network administrator can assign actions to take for such traffic, depending on the needs of the organization. Identifying Microsoft 365 network traffic is the first step in being able to differentiate that traffic from generic Internet-bound network traffic. A step-by-step process that outlines the Session Smart Routing Application Identification is located in the **Session Smart Docs** for Microsoft 365.

The screenshot shows the Juniper Authority configuration interface. On the left is a navigation sidebar with 'Services' selected. The main area displays a table of services. A red box highlights the Microsoft 365 services.

Name	Description	Service Group	Security
_conductor_1			
_conductor_128T-SCUS_1			
Default-Internet			
LAN-Service			
O365-Common	Microsoft 365 Common and Office Online		
O365-Exchange	Exchange Online		
O365-SharePoint	SharePoint Online and OneDrive for Busi...		
O365-Skype	Skype for Business Online and Microsoft ...		

Figure 2: Microsoft 365 services identified by Session Smart Routing

The Session Smart Router can monitor latency, jitter, loss, and loads over these different paths and choose the optimal path for sending Microsoft 365 traffic, thereby guaranteeing performance for those sessions as needed. Selecting the optimal path will help minimize and stabilize latency between users and the Microsoft 365 application. If multiple connections are available, then the Session Smart Router can monitor SLAs over these different paths and direct Microsoft 365 traffic accordingly.

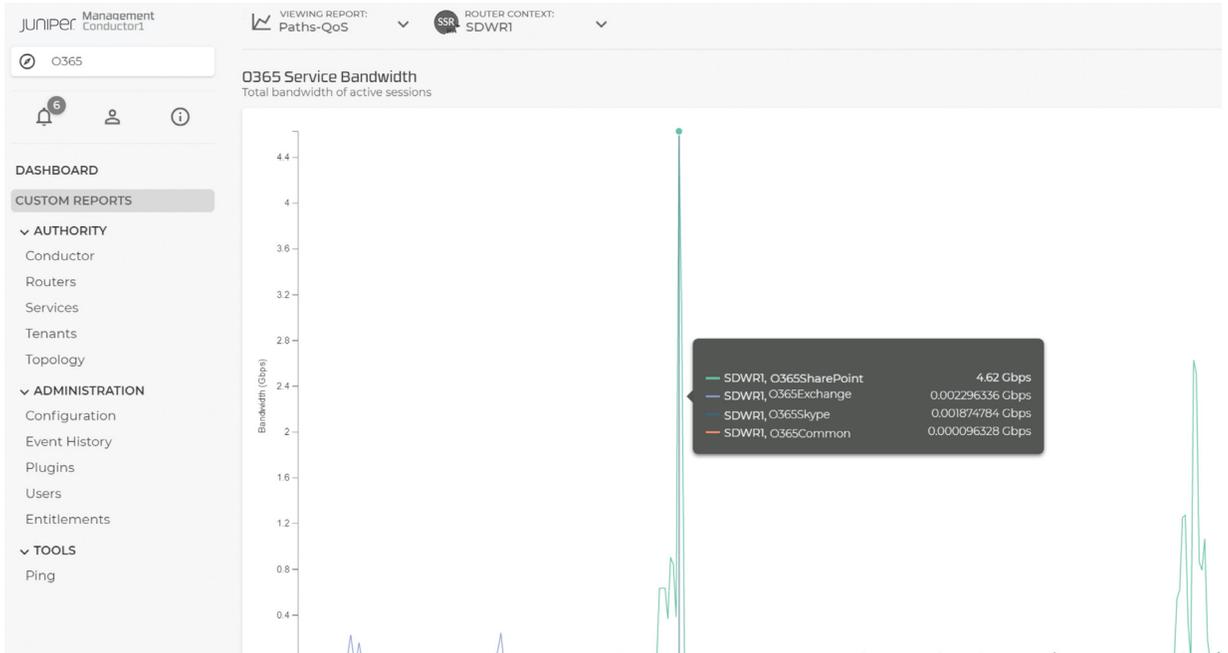


Figure 3: Microsoft 365 application prioritization over Direct Internet Access

Connecting to the closest Microsoft 365 PoP via DIA

Ensuring that users connecting to the nearest Microsoft 365 PoP, whether from an SD-Branch or HQ, is critical to a successful experience. In an SD-WAN deployment, Direct Internet Access (DIA) for Microsoft 365 services should be applied with the highest level of priority to minimize unnecessary latency.

Microsoft operates an extensive global network that includes many front-end servers around the world. In most cases, there will often be a network connection and front-end server close to the user's location. The AI-driven SD-WAN solution does not require VPNs or tunnels to a central location. The tunnel-free solution with no encapsulation ensures that Microsoft 365 traffic can be easily identified.

The Session Smart Router follows a zero-trust security model without requiring backhauling traffic to a cloud security provider. This, in turn, provides users with local Internet egress and local DNS resolution while ensuring the traffic destined for Microsoft 365 can connect to the closest global Microsoft Front Door Servers. Shortening the network path reduces latency and improves Microsoft 365 performance.

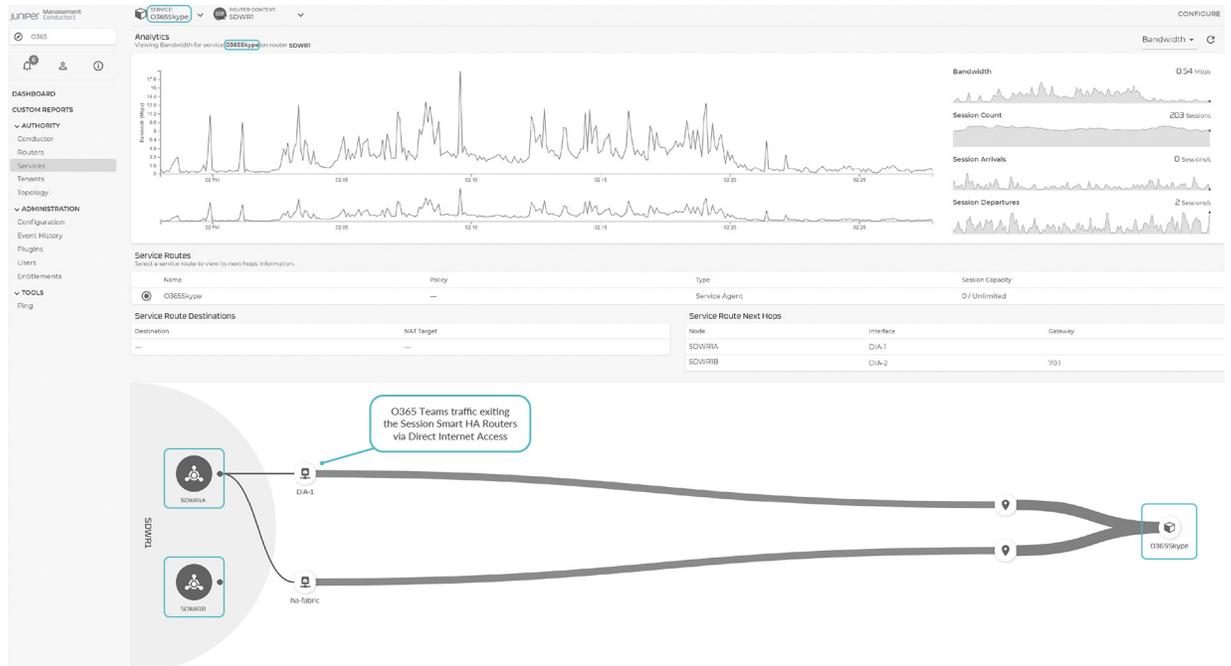


Figure 4: Shows Microsoft 365 Skype for Business/Teams traffic leaving the routers via Direct Internet Access

Customer use case

A financial services customer utilized Microsoft 365 as a collaboration platform for its users and also took advantage of Azure to host many of their internal applications. The customer deployed the AI-driven SD-WAN solution in their on-premises environment, including branch offices and HQ data center, and extended it into Azure. Leveraging SD-WAN to enable secure and local Internet-based egress from user locations was key to solving application performance issues, reducing latency for Microsoft 365, and saving costs on leased MPLS lines. With multiple branch offices, a main Datacenter and a footprint in Azure, the customer removed their leased lines and leveraged Internet bandwidth, Secure Vector Routing, and AI-driven SD-WAN from Juniper Networks.

The less expensive direct Internet lines used for circuit failover were leveraged for the highest priority and session state routing for Microsoft 365 applications. All other non-Microsoft 365 traffic was sent over the Internet with no tunnels, instead, using Secure Vector Routing to the main HQ data center. Traffic to Azure applications was sent using Secure Vector Routing to Azure. This new digital transformation architecture enabled substantial economic savings, better performance for Outlook, OneDrive, SharePoint, and Teams, and provided connectivity to Azure applications while saving on bandwidth costs.

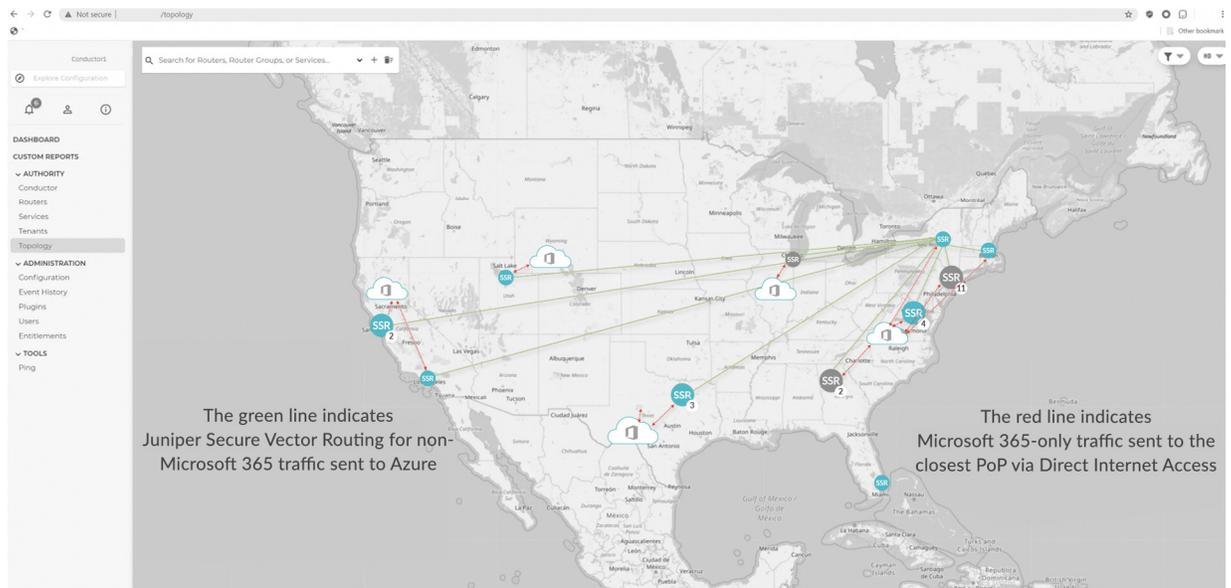


Figure 5: Session Smart Conductor management portal managing multiple branches with each branch having Direct Internet Access to send Microsoft 365 traffic to the closest PoP. Each branch is connected to the Azure head-end router via standard ISP circuits with Secure Vector Routing and no tunnels

Summary

The Juniper Session Smart Router can automatically identify Microsoft 365 traffic dynamically and efficiently. Based on policies set by the network administrator and the connectivity options available, the Session Smart Router can ensure that Microsoft 365 traffic is sent over the best possible paths with the least amount of latency. Ensuring that crucial workload traffic for Microsoft 365 has higher priority over low-value traffic verifies the best end-user experience. Networks can get congested, and Internet links can suffer. It matters what the router does during those critical periods to provide an optimal experience to the end-user. Juniper Session Smart Routers are built to deliver exceptional SaaS and Microsoft 365 experiences from any location.

About Juniper Networks

Juniper Networks is 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. Additional information can be found at Juniper Networks (www.juniper.net) or connect with Juniper on [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
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

