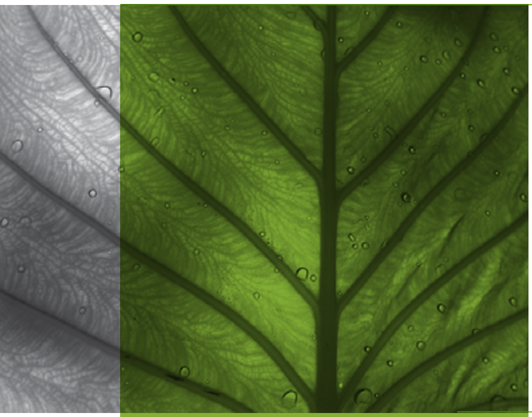

MAXIMIZING MICROSOFT AZURE EXPRESSROUTE DIRECT PERFORMANCE WITH AI-DRIVEN SD-WAN

A Microsoft Azure Cloud Solution with High Throughput Gains on Encrypted Traffic

Challenge

Microsoft Azure ExpressRoute improves cloud/DC application performance by letting enterprises create high speed private connections between Azure data centers and on-premises or colocation infrastructure. IPsec encryption is optionally offered for security or compliance reasons, but this can greatly impair performance.

The challenge for enterprises is to maximize Azure ExpressRoute bandwidth for a better user experience while securing those workloads with encryption.

Solution

Juniper's AI-Driven SD-WAN uses Adaptive Encryption on demand or full encryption for workloads without the overhead of IPsec. While encrypting application traffic, the session-oriented nature of Session Smart Routing (SSR) detects whether the traffic is already encrypted. If application traffic is already encrypted, the router won't re-encrypt the packet, thus eliminating the overhead of double encryption.

Benefits

- *Superior throughput of encrypted traffic: 9Gbps on a 10Gbps link*
- *Simplifies the network transport layer in Azure with fewer Network Virtual Appliance (NVA) VMs and no tunneling*
- *Session Smart Routing saves up to 30% in bandwidth costs*
- *Adaptive Encryption for already-encrypted workloads saves CPU overhead*
- *Easier VM migration to Azure by maintaining the same IP addresses using Overlapping IP Addresses*

Introduction: Microsoft ExpressRoute Direct for the Cloud-Connected Network

As organizations adopt and migrate their workloads to the Microsoft Azure Cloud, network connectivity plays a strategic role in the overall experience for cloud-enabled workloads. As opposed to the public Internet, customers benefit from a private circuit—such as ExpressRoute Direct—to transport their data to Azure.

ExpressRoute Direct provides dual 100 Gbps or 10 Gbps connectivity, and supports Active/Active connectivity at scale. This allows enterprises to connect directly into Microsoft's global network at peering locations strategically distributed around the world.

At times, customers need encryption for regulatory compliance or for other security reasons. The standard approach to achieve this is to use IPsec, a suite of protocols that establish a traditional tunnel to apply encryption to data in transit to Azure.

Some SD-WAN solutions that provide a cloud-connected solution with IPsec use encapsulation and encryption; however, this may come at the cost of bandwidth reduction. When used in tunnel mode, the bandwidth reduction can be attributed to the Encapsulation Security Protocol (ESP) portion of IPsec. The overhead of encapsulation reduces bandwidth by up to 30% or more and often leads businesses to choose not to encrypt traffic in order to maximize throughput for cloud workloads.

> *"In our recent testing of the Juniper SSR solution with a 10Gb ExpressRoute Direct circuit, we were able to securely deliver up to 9Gb of encrypted throughput with less overhead than IPsec. This results in more throughput for our customers that need end-to-end encryption for their workloads moving to Azure."*
>
> *– Jon Ormond, Principal Program Manager – Azure Networking Engineering, Microsoft Corporation*

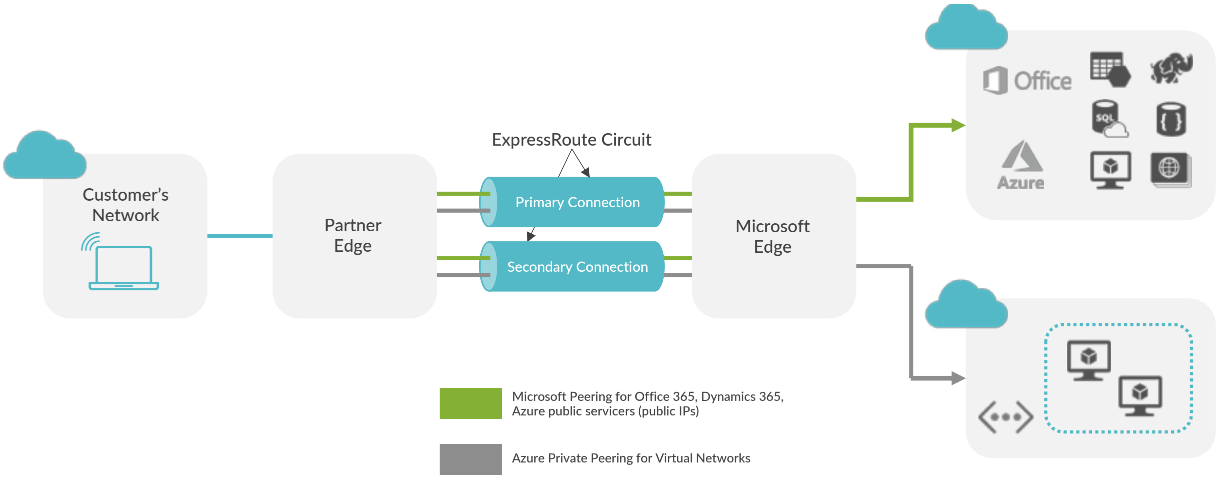
Customer's Network
Partner Edge
ExpressRoute Circuit
Primary Connection
Secondary Connection
Microsoft Edge
Office
Azure
SQL
Microsoft Peering for Office 365, Dynamics 365, Azure public servicers (public IPs)
Azure Private Peering for Virtual Networks

Figure 1: ExpressRoute Direct (Source: Microsoft)

Key Features

Microsoft Azure ExpressRoute Direct allows customers to connect directly into Microsoft's global network at peering locations strategically distributed around the world. ExpressRoute Direct can provide up to dual 100 Gbps connections, which supports Active/Active connectivity at scale (Figure 1).

The solution defines circuits (primary and secondary connections) between the customer (or partner) edge and the Microsoft Edge to the Azure Cloud.

Key features that ExpressRoute Direct provides include:

- Massive data ingestion into services like storage and Cosmos DB
- Physical isolation for industries (such as banking, government and retail) that are regulated and require dedicated and isolated connectivity
- Granular control of circuit distribution based on business unit
- Large scale throughput of 10 Gb to 100 Gb of connectivity

Supporting Compliance Requirements

Businesses that use ExpressRoute Direct for private transport may require encryption for regulatory or compliance reasons. As ExpressRoute Direct uses private circuits dedicated to each customer's tenant, encryption is (by default) disabled over these circuits. This can help to maximize bandwidth.

Applying encryption over ExpressRoute Direct is typically achieved by using IPsec tunneling, and can be complicated to design, difficult to scale, and costly to operate. Juniper's AI-driven SD-WAN solution is a session-based workload routing architecture that can improve this scenario by providing encryption without encapsulation overhead, and thus delivers more throughput for cloud connectivity.

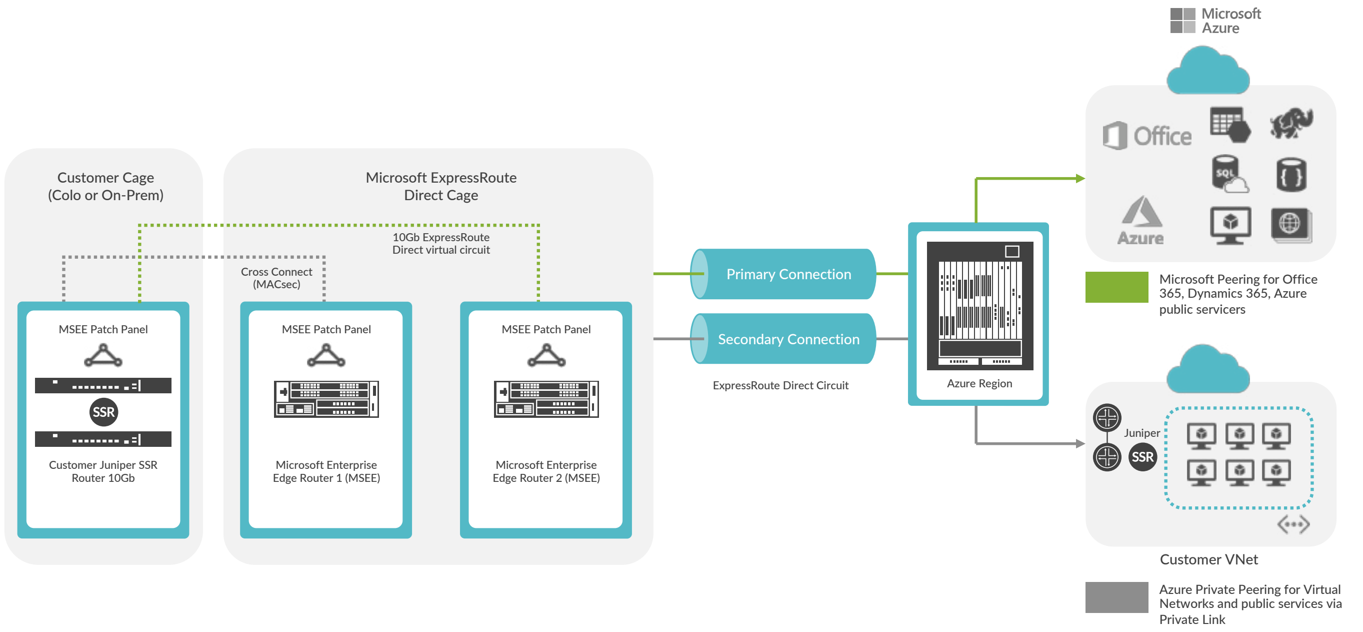
Microsoft Azure
Office
Azure
Microsoft Peering for Office 365, Dynamics 365, Azure public servicers
Customer Cage (Colo or On-Prem)
Microsoft ExpressRoute Direct Cage
10Gb ExpressRoute Direct virtual circuit
Cross Connect (MACsec)
MSEE Patch Panel
SSR
Customer Juniper SSR Router 10Gb
MSEE Patch Panel
Microsoft Enterprise Edge Router 1 (MSEE)
MSEE Patch Panel
Microsoft Enterprise Edge Router 2 (MSEE)
Primary Connection
Secondary Connection
ExpressRoute Direct Circuit
Azure Region
Juniper
SSR
Customer VNet
Azure Private Peering for Virtual Networks and public services via Private Link

Figure 2: Juniper SSR with ExpressRoute Direct

Using Juniper SSR to Optimize ExpressRoute Direct

When using Juniper SSR in an ExpressRoute Direct environment, the SSR instances connect to Microsoft Enterprise Edge (MSEE) routers over 10 Gbps connections. The MSEE routers then create the ExpressRoute Direct circuits into Azure regions, which may be dedicated to peering for Microsoft services or may house other public or private services in a customer VNet (Figure 2).

The Microsoft hardware is in the ExpressRoute cage, while the Customer cage contains the Juniper SSR customer-facing components. The Juniper SSR is dedicated to customer connectivity.

Customers can choose which SSR VM instance in the Azure Marketplace they need to scale up to 10 Gbps. This part of the solution is managed by the customer and is shown here to illustrate the end-to-end Juniper connectivity.

Some of the unique features of SSR are well suited to the Azure environment. For instance, encryption with SSR has very high throughput compared to IPsec: users see 9Gbps of throughput on a 10Gbps link. This is not possible with IPsec. Furthermore, to simplify connectivity, customers can maintain the same IP addresses on-premises and in Azure. Learning Virtual Routing and Forwarding (VRF) Routes and maintaining IP addresses for each VRF instance helps customers simplify the process of migrating VMs in the same address space. This can lead to a huge time savings when migrating VMs from on-premises to Azure as there is no need to modify IP and DNS entries to assure proper segmentation during the migration.

Finally, the solution also supports Azure Accelerated Networking, which enables Single Root I/O Virtualization (SR-IOV) to a VM. This high-performance option takes the physical host out of the data path, thus reducing latency, jitter, and CPU utilization. When SSR is used in this environment, network traffic arrives at the VM's network interface (NIC), and is then forwarded to the VM. Network policies are also applied in hardware, which enables the NIC to forward traffic directly to the VM, while maintaining the policies it would have otherwise applied in the host or the switching infrastructure.

Further Optimizations with AI-driven SD-WAN

Juniper AI-driven SD-WAN enhances this solution by providing agile, secure, and resilient WAN connectivity with breakthrough economics and simplicity. The colocation and Azure cloud facilities shown in Figure 2 can of course be instances of the cloud and data center locations shown in Figure 3.

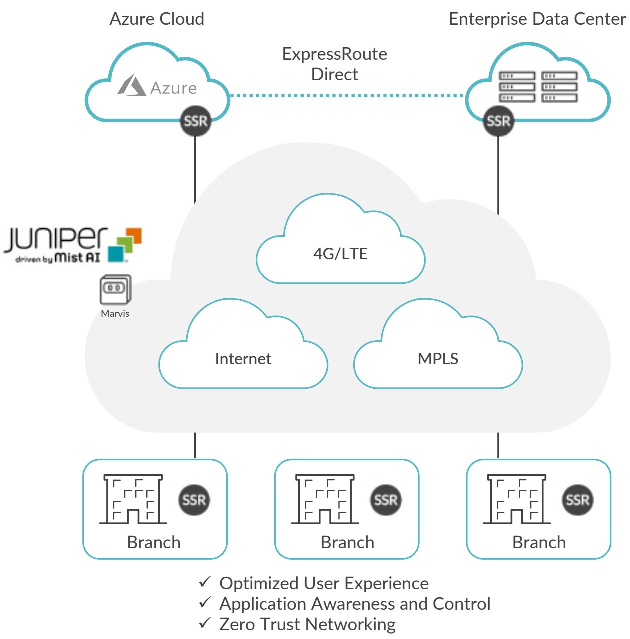

Figure 3: AI-driven SD-WAN

Using Mist AI Cloud and the Marvis Virtual Network Assistant, this solution optimizes for user experience, with guaranteed application performance, instant failover for all applications, and continual insights with recommended actions. For instance, AI-driven SD-WAN can tune the network based on whether performance issues are related to applications, devices, or WAN links. This ensures that the ExpressRoute Direct circuits are also used optimally.

Summary

Juniper SSR and AI-driven SD-WAN, integrated with Microsoft ExpressRoute Direct, allows enterprises to achieve an unprecedented increase in bandwidth, guaranteeing a major increase in throughput while still ensuring traffic is encrypted.

Traditional IPsec solutions connecting to Azure have limitations and require more complicated tunnel designs as well as more infrastructure VMs, while at the same time lacking the simplicity of this integrated solution.

For More Information

- Session Smart Routing – How it works
- Juniper AI-Driven SD-WAN Demos
- Juniper's AI-driven SD-WAN
- Juniper Public Cloud Partnerships

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

Juniper Networks | Driven by Experience™