SD-WAN for Optimal Office 365 Connectivity and Performance

Evolving Needs for WAN Network Architecture

Enterprise networks have historically been architected to provide users access to applications and data hosted in private data centers. For Internet traffic, the WAN network can act as a gateway for access to the Internet but, because of security requirements, the resulting large networking security stack is typically hosted in the remote datacenter.

As a result, Internet traffic for branch offices is often backhauled over the WAN and centralized in the datacenter. This model was necessary and worked well for providing access from users within the branch to on-premises centralized apps such as email and document sharing. For traditional Internet browsing, this centralized model with remote security stack was also adequate, as the performance and scale demands of recreational Internet use were moderate at best.

As enterprise adoption for mission critical, high performance SaaS apps such as Office 365 at scale continues to increase and employees are more distributed, the traditional method of backhauling traffic to centralized hub locations for network egress/breakout creates high latency and congested links leading to a poor user experience. Applying traditional network security inspection controls including inline decryption of traffic on complex SaaS protocols used by Exchange Online, SharePoint Online, and Teams is not at all effective. It often leads to unnecessary overhead and performance bottlenecks, causes interoperability problems, availability issues, and in many cases supportability challenges. In addition, backhauling both SaaS and enterprise applications over traditional network architectures like MPLS is costly and adds complexity.

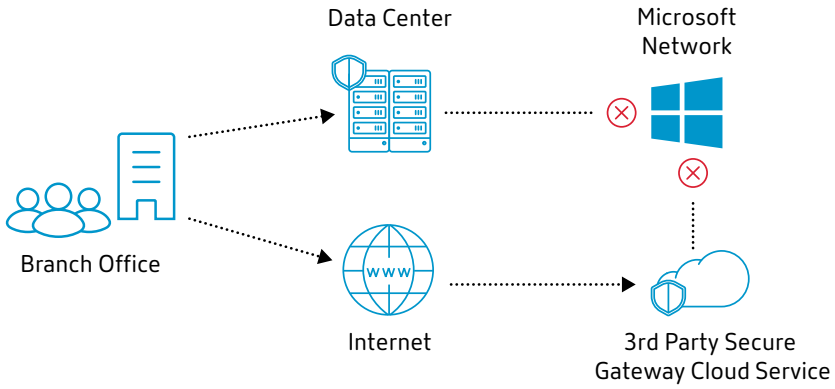
Improving Branch Office User Experience with Microsoft

In order to minimize latency caused by backhauling traffic through the datacenter, organizations can enable direct Internet breakout of Office 365 application traffic from office locations. This also frees up WAN links for other traffic.

Microsoft's concept brings their services as close to their customers' users as possible by directing connections to the nearest front door of their Office 365 services. These front doors have a significantly wider geographic reach than the limited set of data centers where the data for a particular user is stored and replicated. As part of the Microsoft cloud, over 130 edge nodes, or points of presence (POPs), stretch across the world allowing customers to connect into the nearest Office 365 entry point. The edge node performs many tasks for network and application experience optimization before the requests are relayed to the data center where user data is located.

Office 365 service front doors do not need to be where back-end Office 365 servers are located; the choice of front door can and should be as close to the office location as possible to provide the best user experience. In addition,

WAN Network Challenges with Office 365



Microsoft peers with 2,700 ISPs globally across more than 190 locations to streamline traffic and reduce the distance it must travel before reaching Microsoft's network.

The ability to identify Office 365 traffic means that other Internet traffic and traffic to other customer destinations can be handled according to customer policies and doesn't have to be tightly coupled with Office 365. This allows a very attractive concept where network connections are routed and handled in accordance with business policies, trust level in the application itself, user experience requirements, etc. For example, a customer may want general Internet browsing traffic or unknown application traffic to be forwarded to a Secure Web Gateway, cloud proxy, or remote datacenter, while trusted Office 365 traffic for Exchange Online can be routed locally and directly to Microsoft over the Internet and secured with Office 365's native security features. This ability to quickly identify key connections and treat them at the network level in accordance with business- and application-centric logic is the key differentiator of the SD-WAN technology.

SD-WAN "Works with Office 365" Support of Microsoft Office 365 Connectivity Principles

Many SD-WAN solutions have been independently tested and is proven to work with Microsoft in support of its Office 365 Connectivity Principles to provide reliable connections directly from office locations to the nearest Office 365 front doors. The "Works with Office 365" designation attests to this qualification of the product under the Microsoft Office 365 Networking Partner Program. The Microsoft Office 365 Endpoints web service publication provides Microsoft's Office 365 endpoint URLs and IP addresses. With support for Microsoft APIs, several SD-WAN solutions use endpoint data to enable direct Internet routing of trusted, latency-sensitive traffic from the branch to Office 365 front doors.

Many SD-WAN vendors can identify and classify Office 365 traffic on the first packet and then steer it to the nearest Office 365 point of entry giving customers the most optimal overhead-free approach that is gated only by the laws of physics. SD-WAN's traffic steering and monitoring capabilities provide easy policy administration of Office 365 detection on the first packet to enable local egress and visibility into the flow.

Case in Point

In remote offices, a leading lighting, communications, and electrical equipment supply company, noticed 40-50 milliseconds of latency was resulting in slow Office 365 application performance even with direct (but not Office 365 optimized) branch breakout because the traffic was being sent to from Amsterdam to the Microsoft edge site in Helsinki.

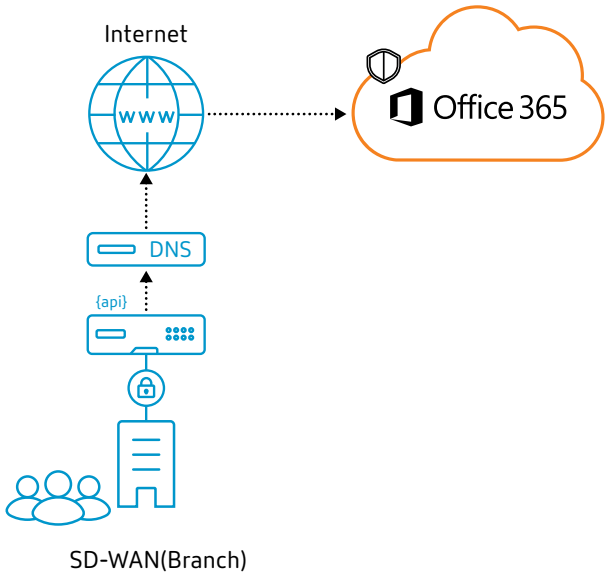
Using the Microsoft API and connectivity principles for Office 365, SD-WAN can identify and optimize trusted Office 365 traffic and direct it to the edge nodes closest to the remote sites. What's more, its TLS encryption ensures security of the data between the remote sites and the Office 365 cloud while SD-WAN can steer untrusted and other types of traffic back to the data center. By implementing SD-WAN the company delivered an 80% reduction in latency for Office 365 access. The result has been a significant improvement in user experience.

"With SD-WAN for Microsoft Office 365, we can create a new office anywhere in hours, not weeks or months. All we need is an Internet connection and a laptop." -Company, CEO

"When we turned on the SD-WAN for Office 365, our traffic started going to Amsterdam, latency went to below 10 milliseconds and we noticed significant user experience benefits." -Company, CIO

There is no need to send trusted traffic through a secure web gateway, as Microsoft provides Office 365 native security features to reduce the network security risk including Data Loss Prevention, Anti-Virus, Multi-Factor Authentication, Customer Lock Box, Advanced Threat Protection, Office 365 Threat Intelligence, Office 365 Secure Score, Exchange Online Protection, and Network DDOS Security. Eliminating hairpinning of key Office 365 experiences through remote cloud datacenters, network security virtual appliances, proxies, and secure web gateways in favor of direct routing from user location directly to

Local Egress of Office 365 using SD-WAN



the Microsoft network is one of Microsoft's key recommendations for minimizing latency and improving user performance with Office 365 SaaS applications.

Managing Bandwidth Through URL Categorization

The URLs requiring the highest amount of optimization create the largest load on the network links, negatively impacting performance. To provide a more optimized path with direct egress, URL categorization helps provide policies for directing traffic to the appropriate endpoints to reduce the network bandwidth challenges. Therefore, URLs are now categorized into the following three groups to help customers deal with the endpoints in specific ways according to the needs of the endpoint and the business.

1. **Requiring an Optimized Path**
   A small number of endpoints require low latency unimpeded connectivity, which should bypass proxy servers, network SSL break and inspect devices, and network hairpins. Even though a very small number of URLs actually require the highest levels of optimization, they account for 75-90% of Office 365 bandwidth, connection, and transaction count. These core endpoints will put massive load on traditional proxy infrastructure and/or require an optimized path provided by direct egress.

2. **Needing Low Latency Unimpeded Connectivity**
   A larger number of endpoints benefit from low-latency unimpeded connectivity. Although not expected to cause failures, it is recommended to bypass proxy servers, network SSL break and inspect devices, and network hairpins. Good connectivity to these endpoints is required for Office 365 to operate normally.

3. **Directed by Default**
   Other Office 365 endpoints can be directed to the default Internet egress location for the organization's WAN.

   To further reduce latency caused by DNS requests to a DNS server that is farther away or busy, ensure that Microsoft connects your clients to resources based on their location with local ("proximate") DNS resolution. To reduce the time to query a DNS server to find out where the actual tenant is, SD-WAN in the branch can perform DNS locally or, if using a cloud proxy, perform DNS at the proxy.

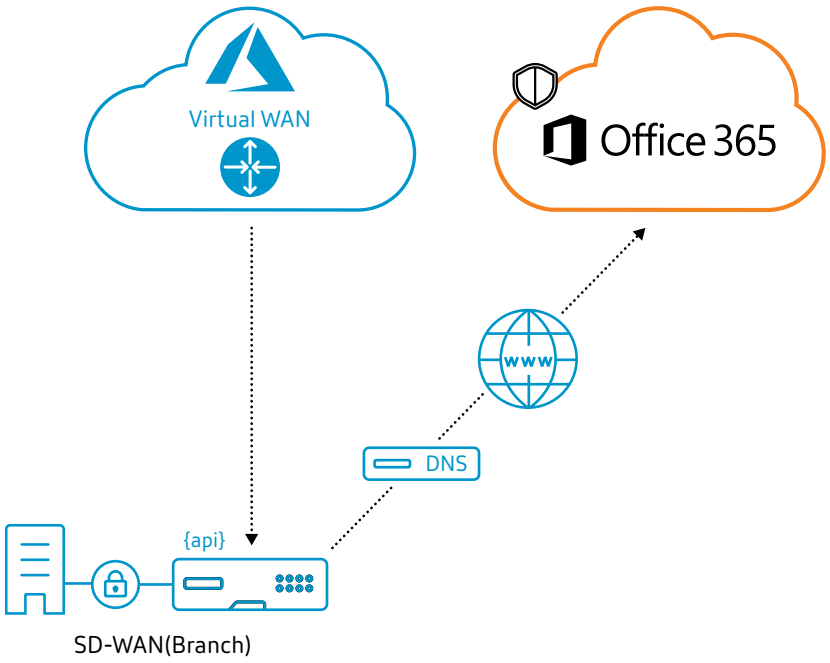
Office 365 Policy Support for Azure Virtual WAN Customers

For Office 365 customers who also use Microsoft Azure Virtual WAN, Some SD-WAN vendors can obtain Office 365 policy settings directly from Azure Virtual WAN via Microsoft's REST API. SD-WAN can leverage these policies from Azure to split the traffic locally, provide categorization to either optimize (for select URLs) or allow, and then egress to the nearest Office 365 front door. SD-WAN provides enterprises the ability to do local breakout of all their Office 365 traffic for all their branches simultaneously to minimize latency.

Ease of Deployment

SD-WAN makes Office 365 networking optimization extremely easy to deploy through a combination of automation and simplified configuration. Selected SD-WAN vendors can offer a fully automated solution, REST API integration, automatic creation of all the necessary low-level DNS and data traffic-steering policies, PAC file modifications, and NAT and firewall rules.

Azure Virtual WAN and SD-WAN Integration



A simple, easy-to-use screen provides top-level configuration to enable Office 365 optimization with various connection options for local breakout. The simple configuration and sophisticated backend functionality reduce the time it takes to get up and running.

Innovative networking ideas offers customers a modern SD-WAN solution to make it easy to adopt those principles and optimize the branch office user experience for latency-sensitive Office 365 applications.

PCS TECHNOLOGY CONSULTANTS

Contact: PCS Technology Consultants, LLC
Phone: 678-799-7861
Email: Info@PCSTechConsultants.com