Accelerate Microsoft 365 with Versa Secure SD-WAN

Traditional Enterprise Network challenges with Microsoft 365 SaaS Applications

Enterprises around the world have adapted multi-cloud technologies like Infrastructure as a Service (IaaS) and Software as a Service (SaaS) solutions from different providers to host their applications. The rapid pace of digitization has only accelerated this move to the cloud. Microsoft 365 is a leading Enterprise suite of business applications that is SaaS based and used by several businesses around the world. The workforce and the applications being more distributed today has created two particularly contradictory requirements for the network and security administrators:

1. The users require the same user experience with any of the Microsoft 365 application just as any other application that is hosted in a on-premises datacenter.
2. Remote users and Internet based applications have created additional threat vectors which need additional scrutiny of all Internet bound traffic.

The security perimeter approach requires that all Microsoft 365 SaaS traffic from the branch is coupled with the regular Internet traffic and backhauled to the Hub or a Secure Web Gateway for security inspection. This adds latency which not only impact throughput but also degrades the user's experience with these applications.

Latency in this scenario is primarily impacted by the following factors:

- Propagation delay from the branch office to the Hub or Gateway.
- Processing delay due to the intermediate processing of the traffic by the network and security appliance stack at the branch and the Hub or Gateway.
- Queuing delay due to traffic congestions.

The lack of visibility is also a concern as the Network Administrator cannot properly differentiate the Microsoft 365 business from casual Internet browsing traffic. It hinders the ability to provide any kind of traffic prioritization in the network. Even within the Microsoft 365 suite of applications, some collaborative applications like Teams and SharePoint Online may require different prioritization than applications like Exchange Online. Also since this traffic cannot be easily differentiated, the same intrusive security policies have to be applied for all Internet bound traffic; resulting into a degraded user experience.

The user traffic to the Internet for both business and non-business usage has increased exponentially in the recent years. Bandwidth intensive applications (sharing large files, high definition video etc.,) increases congestion not only at the branch office but also at the Hub or Gateway site. Adding more capacity to the MPLS WAN circuits to backhaul all this Internet traffic to the Hub or Gateway is not only expensive but also not scalable. To overcome the reliance on expensive MPLS circuits, Enterprises now use Internet WAN links at branch sites and implement SD-WAN solutions like Versa's Secure SD-WAN to provide an encrypted overlay for VPN connectivity with local Internet breakout for specific SaaS applications like Microsoft 365.

Enhanced Microsoft 365 user experience with Versa Secure SD-WAN

Microsoft 365 is a globally distributed SaaS application widely used by enterprises for applications that enable real time communications, collaboration, file sharing, email etc. These applications are very critical for business operations and seamless connectivity to them is extremely important. The best performance is typically achieved when these applications are accessed over low latency direct Internet access (DIA) path from the branch where the user is connected from.

To ensure best user experience, Microsoft has published the following Microsoft 365 network connectivity principles - https://docs.microsoft.com/en-us/microsoft-365/enterprise/microsoft-365-network-connectivity-principles?view=o365-worldwide.

- Identify and differentiate Microsoft 365 traffic using FQDN/IP/Ports.
- Egress network connections locally with matching DNS resolution
- Minimize latency and avoid network hairpins
- Eliminate intrusive network security

Versa Networks Secure SD-WAN is an industry leader SD-WAN and Security solution widely used by Enterprises across all verticals to securely connect their users at the branch with their application workloads. The Versa Secure SD-WAN solution offers an advanced suite of features that enables a secure and optimal connection between the user and the application, irrespective of where the application is placed i.e., on-premises, public cloud hosted or SaaS. This allows the Enterprises to confidently accelerate their digital transformation to a multi-cloud era with the network functioning as an enabler to this transformation. Versa Networks partners with Microsoft to implement the Microsoft 365 Network Connectivity Principles to ensure that Enterprises benefit from the advanced traffic steering capabilities of the Versa Secure SD-WAN solution to get an exceptional user experience for Microsoft 365 suite of SaaS applications.

The Versa Operating System (VOS) software running on the branch appliance features Advanced Routing, Traffic steering and Network Security built into the same software stack. This gives the Enterprises IT administrators maximum flexibility in applying policies tailored to their business needs using a single pane of glass for managing both the SD-WAN and Security related configuration. The Graphical User Interface (GUI) is designed to be simple and intuitive with a high focus on automation using a template driven approach that allow reusability of configuration objects. Deep and powerful AI driven traffic insights including Application Performance Management (APM) is provided using the Versa Analytics software that aid in capacity planning, incident management and network diagnostics.

More details about the Versa Secure SD-WAN solution can be found here - https://versa-networks.com/solutions/wan-edge/secure-sd-wan.php.

First Packet detection and local DNS egress for Microsoft 365 Applications

Versa Secure SD-WAN uses the Endpoint information published by Microsoft to detect the Microsoft 365 traffic on the first packet of the session initiated by the client. Even if the first packet in the session is a TCP syn packet which contains no real information with regards to the Application, the Versa VOS can detect the exact Microsoft 365 application by looking at the destination IP address and port number. This enables the Traffic Steering policy on VOS branch to steer the traffic starting with the first packet of the session to a local Internet WAN link. This also ensures that high latency paths are avoided for business critical Microsoft 365 traffic.

The Microsoft 365 service endpoint IPs, FQDNs and port numbers are learnt by the Versa VOS branch software in a dynamic fashion using the APIs published by Microsoft. Any Microsoft updates to the endpoints are then automatically obtained and updated.

Microsoft also stresses the importance of DNS egress path to be the same as the traffic path. This is an important aspect to ensure that the traffic to the Microsoft datacenter always takes the shortest path with the least latency. When the traffic has to egress from a specific Internet WAN circuit, it is important to ensure that the DNS resolver being used is as close as possible to the branch egress (DIA), which may be the ISP-provided DNS servers, customer deployed DNS infrastructure at the branch location, or another DNS solution which is optimized for regional breadth of deployment. This ensures that geographical affinity to the Microsoft 365 frontend datacenter is maintained based on the source IP address of the branch.

Let's say if an Enterprise branch located in the US West region is configured to route the DNS traffic to a Hub site that is located in the US East region. The DNS resolver there would return an IP address for a Microsoft 365 datacenter that is closer and in the same region. So even if the branch in US West is configured to break out the traffic locally the traffic still uses a longer path to reach its destination.

The Versa VOS software has support for DNS proxy. When a client makes a DNS request for a Microsoft 365 application, the system chooses the same path for the DNS request as the actual data traffic path that is specified in the Traffic Steering policy. From the last example, if the branch in the US West region steers the DNS traffic for an Microsoft 365 FQDN to the local Internet WAN link, then the local ISP would likely resolve the DNS request to an IP address from a Microsoft Datacenter that is in the same region. This ensures that the traffic to the Microsoft 365 service always takes a shortest path over the Internet.

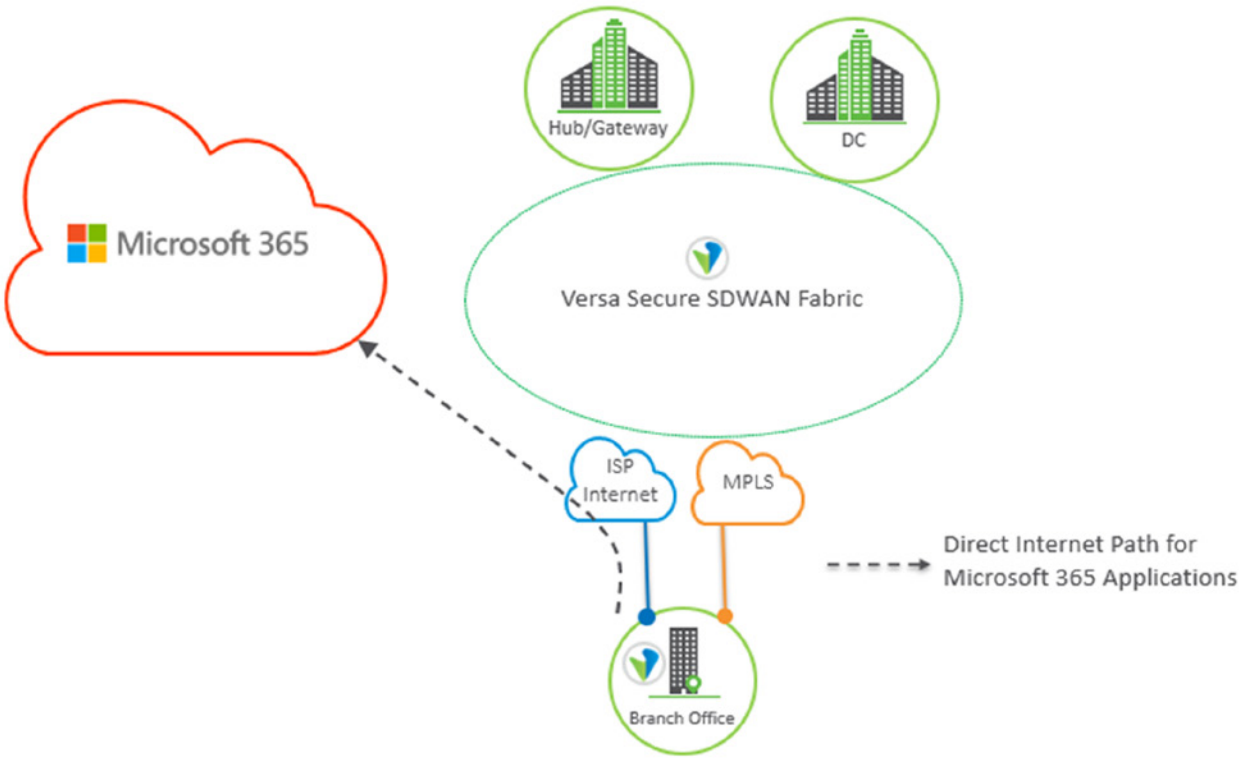
Security for Microsoft 365 Applications

The Versa VOS software has a built in firewall with several advanced Next-Generation and UTM threat prevention capabilities. If the Enterprise is deploying such advanced security inspection at the branch to inspect the Internet bound web traffic, then a stateful zone based firewall rule can be configured to ensure that the Microsoft 365 Optimize and Allow category of traffic is allowed and not inspected by any of the Versa security threat prevention modules. The Microsoft 365 Default category of application can be scanned by the various Versa security threat prevention modules. This is as per the recommendation from Microsoft as specified in the Network connectivity principles for Microsoft 365 applications. More details about the Security functionality in the Versa VOS software can be found here - https://versa-networks.com/solutions/wan-edge/security.php.

Traffic Optimization for Microsoft 365 Applications

Scenario 1 – Static Local Internet Breakout for Microsoft 365 Applications

Some Enterprises maintain a policy of centralized security inspection where all the Internet bound traffic arrives at a Hub or Gateway location to be inspected by a Network Firewall. Having a local Internet circuit at the branch site to break out the critical business SaaS traffic like Microsoft Teams, SharePoint Online, Exchange Online etc., helps to reduces the latency to these applications. Even in the scenario where a PAC file is deployed at the hosts to forward all Internet traffic to the Web Proxy which could be deployed at the Hub or a Gateway site, the Versa VOS branch can selectively break out the Microsoft 365 SaaS traffic at the local branch avoiding the higher latency path to the Hub. In the case of a failure of one Internet WAN circuit, the traffic can fallback to another Internet link like a cheaper broadband connection or an LTE circuit. The traffic can also fallback to a remote hub or gateway site if no local Internet path is available.



Scenario 2 – Dynamic Local Internet Breakout for Microsoft 365 Applications

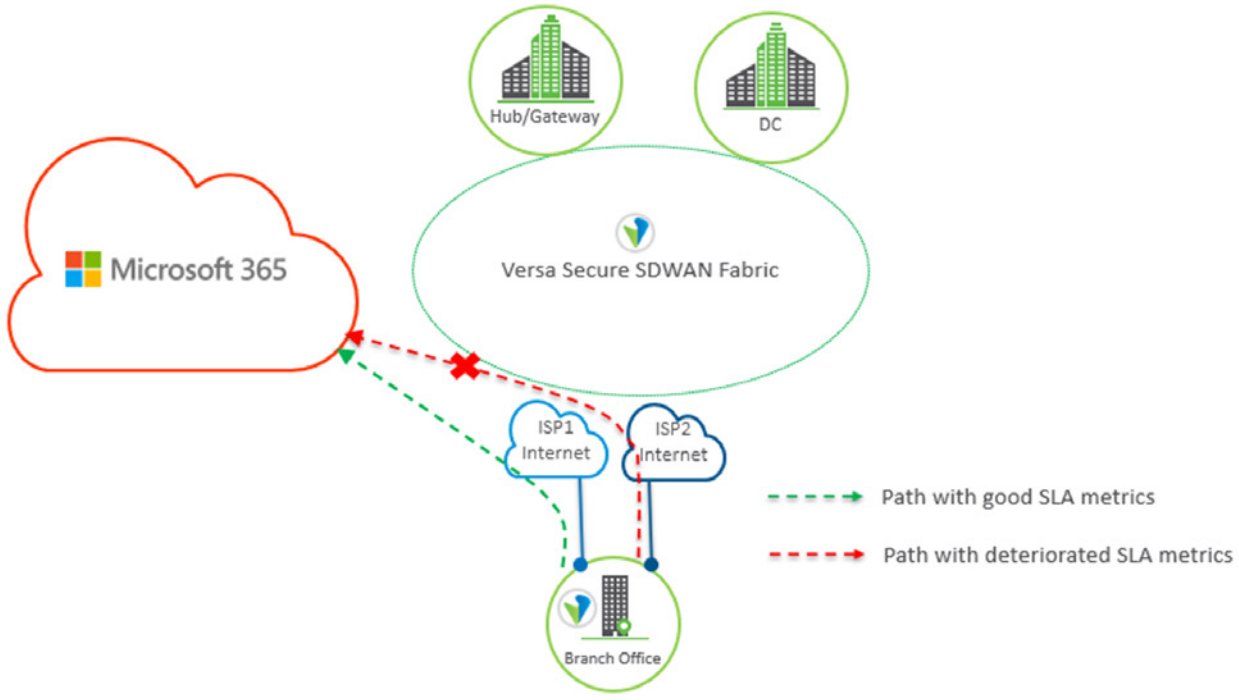
Rather than depending on a single WAN link at the branch, many Enterprises have dual but cheaper Internet WAN circuits at the branch. Routing over the Internet comes without any Quality of Service and hence it is important that the SD-WAN network is also able to do traffic path steering based on the network performance in real time even for web traffic destined to the Internet. The Versa VOS software has specially designed capability to dynamically steer the traffic over the best of the available traffic paths for SaaS applications like Microsoft 365. This can be done in two ways.

a. **Active Monitoring**

Dynamic probe packets to a particular FQDN or IP address can be used to gauge the performance of the WAN path. These probe packets can be ICMP, TCP or HTTP based. Based on these metrics, traffic steering policies can be configured to choose the best WAN path. Microsoft recommends probing the FQDN – http://sdwan.measure.office.com for measuring the performance for Microsoft 365 applications.

b. **Passive Monitoring**

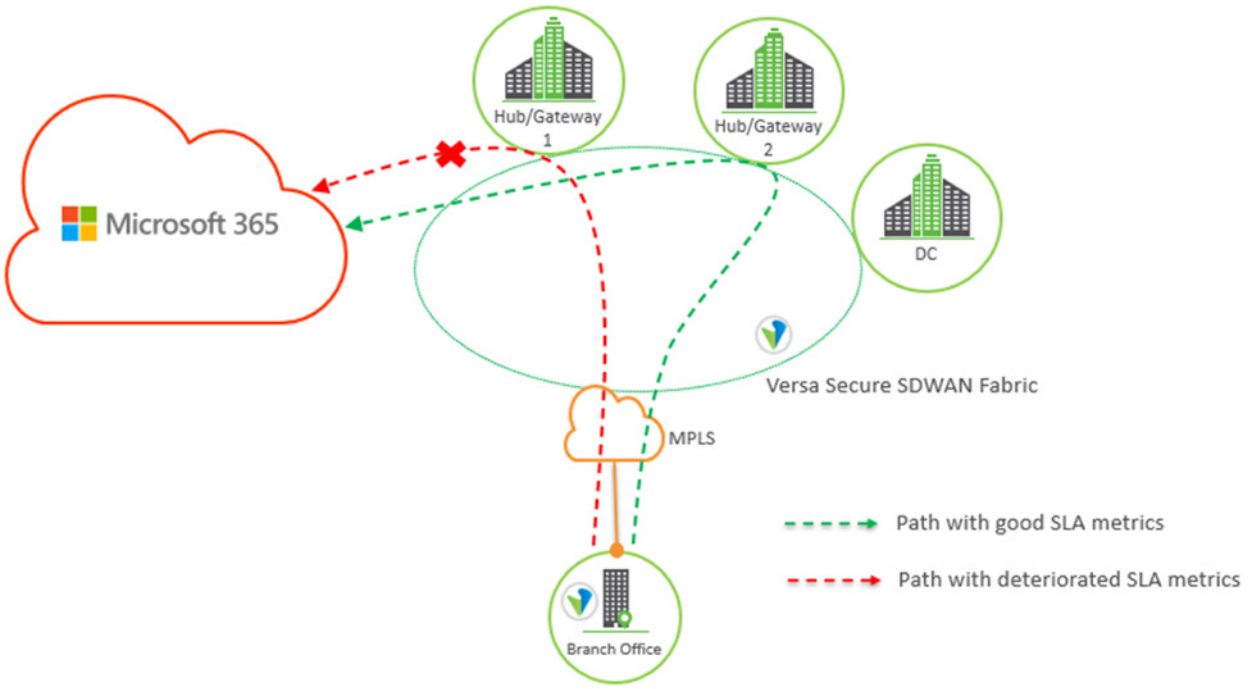
Rather than use active probe packets, the Versa VOS software can monitor the user traffic flows to the various Microsoft 365 applications and rank them based on various performance metrics. This ranking is from a scale of 1 to 100 and is referred to as the Versa Link Rank (VLR). This method of path selection automatically ensures that the business critical Microsoft 365 traffic uses the WAN path with the best performance.



Scenario 3 – Dynamic Remote breakout for Microsoft 365 Applications

Though it is recommended to break out the Microsoft 365 traffic locally from the branch, some Enterprise branch sites still have only MPLS WAN connections and access for SaaS applications like Microsoft 365 has to go through a remote Hub site or Gateway. Usually the branch configuration is setup to prefer one hub site and then fallback to another hub site if the path through the primary Hub fails or the traffic is load-shared across multiple Hub sites. But in a situation where the Internet path through one of the Hub suffers packets loss or high latency due to congestion or any other problems in the path, then the SaaS traffic through this site will suffer deterioration in performance; impacting the access to Business critical applications like Microsoft 365.

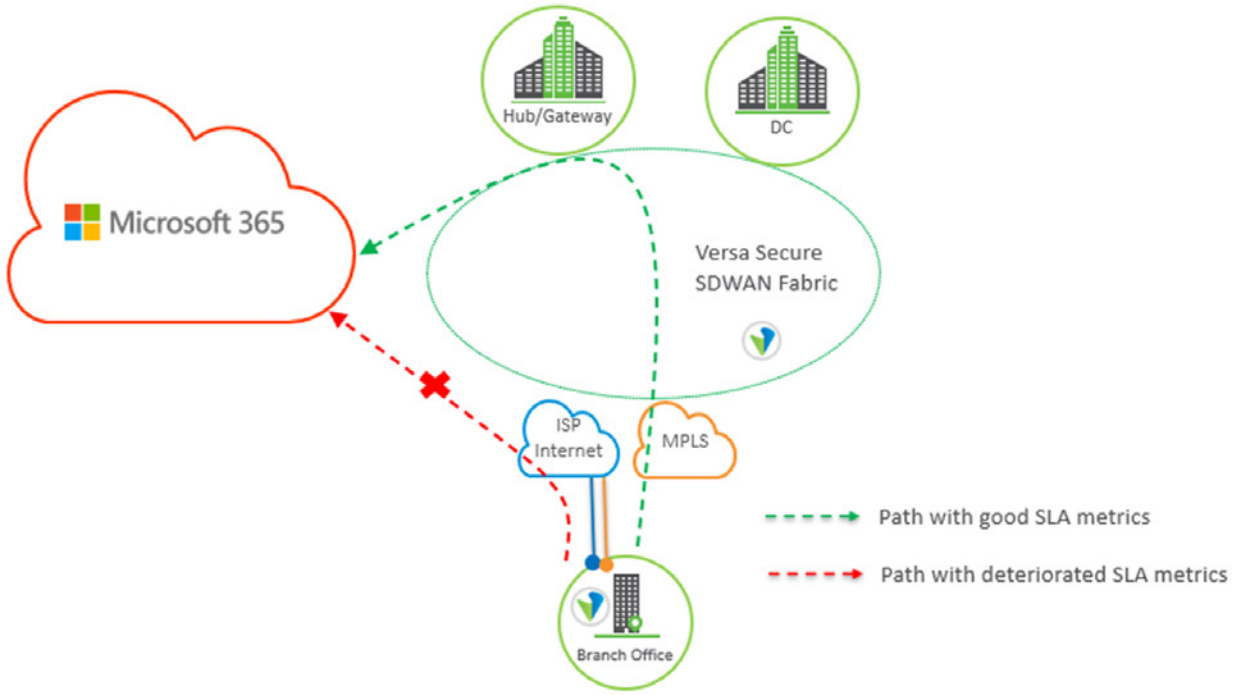
In such scenarios, the Versa VOS software can use both the Active and Passive Monitoring mechanisms described in the Scenario 2 to dynamically select the best performing remote Hub or Gateway. So any brownouts in one of the path can be dynamically detected by the branch and traffic rerouted through an alternate path ensuring that the end user experience with Microsoft 365 applications is not impaired.



Scenario 4 – Dynamic Local and Remote Breakout for Microsoft 365 Applications

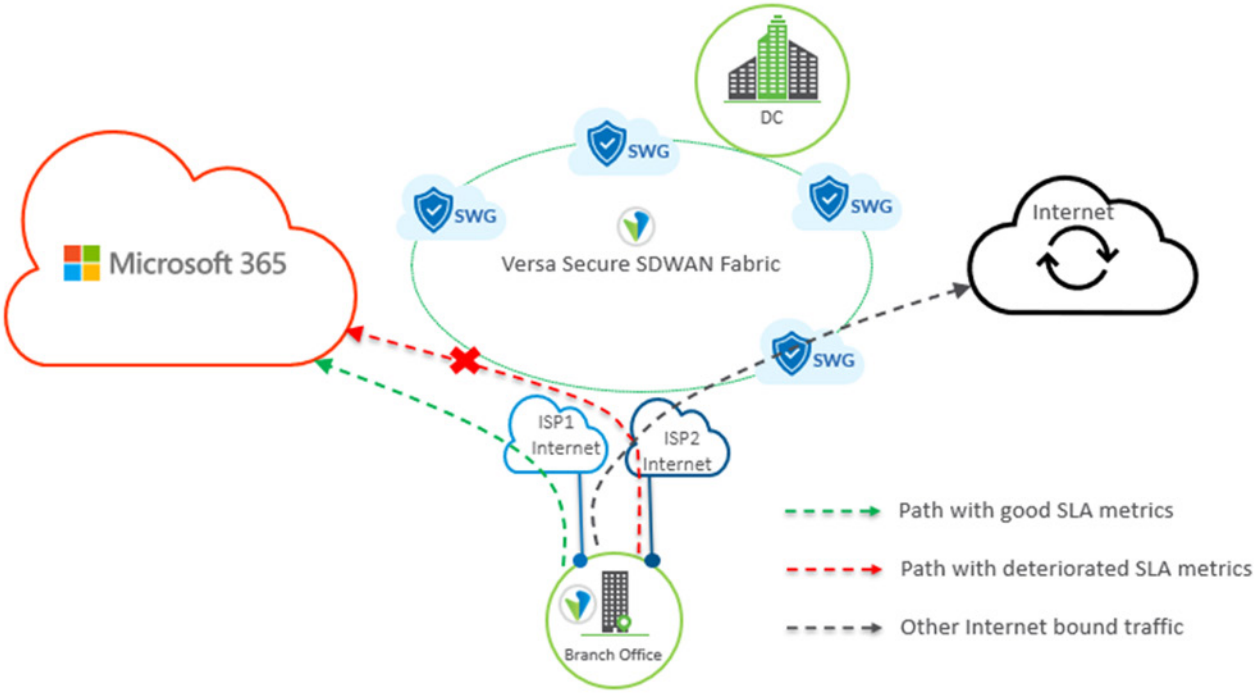
If the local Internet WAN links at the branch suffers a deterioration in performance due to packet loss and/or increase in latency then the Microsoft 365 traffic traversing through this path is bound to get impacted. If the branch has an alternative path to a remote Hub or Gateway offering lower latency and/or packet loss then as described in Scenario 1, this path can only be chosen if the local Internet WAN link is unavailable. But since this is a brownout scenario, the Internet bound Microsoft 365 would continue to be used.

Versa VOS software offers dynamic path selection using Active Monitoring and Passive Monitoring (described in Scenario 2) where the Versa VOS software dynamically choses the best path based on performance metrics like latency, packet loss etc. So in normal circumstances when there is no deterioration in the local WAN link, this path will be chosen. If there is a loss of performance in the local WAN link then the alternate path through the remote Hub or Gateway can be chosen if its path metrics are better.



Scenario 5- Local Breakout for Microsoft 365 Applications with Secure Web Gateway (SWG)

If the Enterprises WAN design consists of using the SD-WAN network for VPN traffic and a SWG for the Internet bound traffic, then a traffic steering policy can be created on the Versa VOS branch to only selectively break out the important Microsoft 365 SaaS traffic like Teams, SharePoint Online, Exchange Online etc. This includes steering the DNS lookup for the Microsoft 365 URL's via the local WAN links. If there is more than one WAN link then the Versa VOS software can dynamically probe the paths as described in Scenario 2 to determine the best path. The other Internet bound traffic can be directed to the SWG for more deeper inspection.



Summary

Microsoft 365 is a business critical SaaS application used by Enterprises worldwide. Versa Networks has collaborated with Microsoft to implement the Network Connectivity Principles for the Microsoft 365 application in its Secure SD-WAN Solution. The Versa Secure SD-WAN solution with its advanced Traffic Steering capabilities, DNS Proxy and First Packet detection capability ensures that users accessing this application always get the best possible performance.

Versa Networks, Inc, 2550 Great America Way, Suite 350, Santa Clara, CA 95054 | Tel: +1 408.385.7660 | Email: info@versa-networks.com | www.versa-networks.com

© 2023 Versa Networks, Inc. All rights reserved. Portions of Versa products are protected under Versa patents, as well as patents pending. Versa Networks and VOS are trademarks or registered trademarks of Versa Networks, Inc. All other trademarks used or mentioned herein belong to their respective owners. Part# SDWANMS365-01.1