**[How To: Optimize Office 365 Network Performance](https://danielchronlund.com/2021/01/20/how-to-optimize-office-365-network-performance/)**

Large (and sometimes small) organisations might find it difficult to deliver great Office 365 performance to users because of network latency or other network related performance issues. The cloud is NOT on-prem and it was built to scale globally. It is important to understand that it is a bad habit to treat cloud security like you do on-prem, with VPN connections, proxy servers and network inspection, because if you do you are disabling all the hard work that Microsoft and other cloud providers has put in to building these hyper scalable content delivery services. I will try to explain what an why you need to do to optimize your Office 365 network connection.

**Office 365 Network Goals**

In this blog post, I will point out some of the most important network optimizations strategies you should use to optimise Office 365 performance for end-users. We do have multiple goals with the optimization:

Diagram

Description automatically generated

As you can see, we are focusing on both the user experience and the security. It’s important to understand that we don’t need to decrease any security just because we’re removing traditional choke points in the network topology. Instead, we can leverage built-in security in the cloud, like Azure AD, Cloud App Security and Microsoft 365 Defender to replace the functionality of VPN and proxy services.

**Office 365 Network Basics**

Office 365 was built to be accessed over the Internet, but Office 365 is NOT the Internet. It’s a SaaS service managed by Microsoft and administered by you. You should always treat it as an extension of your core IT services, not as a “dangerous” Shadow IT service like Instagram or Facebook. Microsoft provides local front doors and peering established with practically every major ISP in the world. This makes the Microsoft global backbone extremely optimized and we want the users to reach this network through the closest front door.

Each Office 365 user can and will establish 32 or more concurrent TCP/UDP connections. This is also something you need to take into consideration if you still want to route the traffic through a traditional choke point service like a proxy server.

**Common Network Transformation Obstacles**

The biggest challenge is often not technical, but political. If IT don’t understand how the Microsoft cloud services work, they are likely not willing to accept this new way of doing security. “It feels better when we route network traffic through a proxy server, firewall or VPN service”.

Another obstacle is company policies that were written before adopting the cloud. They might make it harder to change how you do security but this will in fact slow down the modernisation of security and affect user experience and the overall security posture. Executive sponsorship may be required to get past this obstacle.

Security teams might not be easily convinced that there’s more than one way to accomplish their goals. Here it is important to address the security policies’ goals, rather than their methods.

Applying security measures that were developed and deployed for on-premises services or to control web surfing aren’t going to provide the same level of security assurance, and can have a significant negative impact on performance!

**Office 365 Network Optimization**

Here are some of the most important network optimization strategies for Office 365:

* **Rule #1: Get off your network and onto Microsoft as quickly as possible:**
  + Use localized Internet breakout – Routing your users’ traffic out locally ensures it gets into the Microsoft network quickly with minimum latency.
* **Choke points are bad for Office 365! Avoid:**
  + VPN connections
  + Proxy servers
  + TLS break and inspect
  + Centralized Internet egress
* **Insufficient resources at the edge:**
  + NAT devices may not have enough horsepower (remember that users need around 32 TCP/UDP connections each)
  + Office 365 expects persistent connections
  + If the NAT device is dropping them prematurely, those apps may become unresponsive

This illustrates centralized Internet egress vs localized internet breakouts.

Graphical user interface, diagram

Description automatically generated

**Office 365 Network Connectivity Test**

Microsoft provides a nice tool for testing your connection to Office 365. This tools can be used by any user and it can help with the planning and troubleshooting of Office 365 performance. Try it out on your own computer and compare VPN connection against local breakout.

<https://connectivity.office.com/>

Graphical user interface, application

Description automatically generated with medium confidence

**DNS Resolution Traffic**

How the client resolves DNS is also an important factor. Even the best designed networks can be ruined by poor DNS. Microsoft always returns the response that is closest to the source of the request and that’s why DNS resolution traffic should follow the Internet egress path. It should go out the same path as your users’ Office 365 traffic. This makes sure that you receives the Microsoft IP addresses closest to you. Also, avoid DNS services which may cache results from the wrong parts of the world.

Diagram

Description automatically generated

**VPN Split Tunneling**

VPN doesn’t add any security to cloud traffic. All connections to Office 365 are always encrypted with TLS 1.2 and are very secure in its nature. The illustration below shows that a VPN tunnel just encrypts already encrypted traffic which is unnecessary and performance costly. TLS is what we all rely on for our online banking and it is proved to be secure.

Forcing a TLS connection (or 32 of them) to go over a VPN does not add security, but it does add latency and reduces overall throughput. You should use VPN split tunnelling to exclude Office 365 traffic from the tunnel. There are three categories of traffic for Office 365 (see endpoint categories further down). **Optimize**, **Allow**and **Default.** Optimize and Allow should bypass VPN and proxy, Default can be proxied if required by internal policies.

Diagram

Description automatically generated

**Office 365 Endpoint Categories**

**Optimize** endpoints are required for connectivity to every Office 365 service and represent over 75% of Office 365 bandwidth, connections, and volume of data. These endpoints represent Office 365 scenarios that are the most sensitive to network performance, latency, and availability, like Teams meetings and calls.

**Allow**endpoints are required for connectivity to specific Office 365 services and features, but are not as sensitive to network performance and latency as those in the Optimize category. The overall network footprint of these endpoints from the standpoint of bandwidth and connection count is also smaller.

**Default**endpoints represent Office 365 services and dependencies that do not require any optimization, and can be treated by customer networks as normal Internet bound traffic.

Learn more: <https://docs.microsoft.com/en-us/microsoft-365/enterprise/microsoft-365-network-connectivity-principles?view=o365-worldwide#new-office-365-endpoint-categories>

**Proxy Services**

Do not use a proxy for Office 365 traffic! This is just another unnecessary chokepoint. Common reasons for proxies can be DLP, antimalware or content inspection but these are all already available to you in the service (at scale) and cloud optimized. **Optimize**and **Allow**should go direct and bypass your VPN and proxy. **Default**can be proxied but it is far from necessary.

Graphical user interface

Description automatically generated with low confidence

**Teams Streaming Performance**

Teams uses UDP for streaming traffic including audio, video, and presentation sharing. UDP is more efficient than TCP because if packets are dropped, or arrive out of order, it’s unnoticeable by the user and the stream can just keep going. If UDP is blocked, Teams clients fall back to using TCP.

If a TCP packet is dropped, everything stops until the Retransmission Timeout (RTO) expires, and the missing packet can be retransmitted. If a TCP packet arrives out of order, everything stops until the other packets arrive and can be reassembled in order. Both lead to glitches in audio and video, poor performance and a bad user experience.

This is important! When you force a Teams client to use a proxy, you force it to use TCP! In some VPN solutions, it forces UDP to tunnel through TCP! Both will decrease network performance.

A picture containing text, posing

Description automatically generated

**Learn More**

This is a collection of Office 365 network resources:

[Networking up (to the cloud)](https://docs.microsoft.com/en-us/microsoft-365/solutions/networking-design-principles?view=o365-worldwide)[Microsoft 365 network connectivity principles](https://docs.microsoft.com/en-us/microsoft-365/enterprise/microsoft-365-network-connectivity-principles?view=o365-worldwide#new-office-365-endpoint-categories)[Office 365 URLs and IP address ranges](https://aka.ms/ipaddrs)[Office 365 IP Address and URL web service (for automation)](https://docs.microsoft.com/en-us/microsoft-365/enterprise/microsoft-365-ip-web-service?view=o365-worldwide)[Microsoft 365 Network Connectivity Test](https://connectivity.office.com/)

**Summary**

Remember that the cloud is not on-prem, and it should therefore be treated as a modern cloud service. Cloud services like Office 365 is also not the public Internet and they should be treated as part of your IT, not like Instagram. Follow the guidelines in this article to provide a world class user experience while staying secure by leveraging built-in services like Azure AD Premium, Cloud App Security and Microsoft 365 Defender. I hope this helps!