



The survivor's guide to building an Office 365 network



A Microsoft Office 365 deployment can be daunting. From a fast user experience, to a cost-cutting productivity platform, your users and CIO are expecting amazing things from Office 365. While it's your job to deliver on the promise, you're not going to get very far unless your network has been properly set up for the experience.

Before we get to the good stuff, let's first consider the challenges you're dealing with:

- Your CIO (and more often than not the business itself) has already determined that Office 365 is the solution to all the business's, and the world's, problems.
- If Office 365 fails to scale with your traffic, and users complain about a slow experience, you can bet the responsibility won't fall on Microsoft or your company's executives. Any guesses who'll get the blame?

As you probably realize, getting the network right for Office 365 is going to be a key first step in delivering against the company's goals and expectations. The intent of this guide is to help you identify Microsoft's key recommendations in regards to Office 365 networking, and detail what additional network and security challenges you might face before, during, and after deployment. Taken together, along with Zscaler's perspective as vendor that has helped hundreds of organizations of all sizes successfully deploy Office 365, you might very well come to the conclusion that Office 365 is not that daunting after all.

The Office 365 network challenge

One of the key challenges with Office 365 is that it bucks network conventions that have been in place for 30 years. In spite of mobility trends and increased cloud adoption, many organizations continue to leverage network and security architectures designed for an environment of the past, when applications were all housed in the data center and users rarely left the network. As a result, IT leaders are struggling to provide the fast, seamless experience Office 365 users want and the productivity results management demands.

To successfully build an Office 365 network that performs and scales to your organization's needs, you have to break free from the hub-and-spoke network and centralized gateway approach to connectivity.

As we look to build an Office 365 deployment that will scale and perform, let's consider what our primary goals and objectives should be.

Objectives (business outcomes)

- Create new efficiencies for the business, thereby enabling further agility and wealth creation on shorter timelines.
- Lower the overall IT-related security and compliance risk to the organization.
- Become more adept at deploying well-established, large-scale, cloud-based platforms.

Metrics

- Certify that IT staff is familiar with deployment best practices, standards, and documentation.
- Validate that < 30ms of latency is achievable from all locations, including branch offices, at all times with respect to Office 365 traffic.
- Validate that there are no "surprises" once the deployment commences, such as security appliances or networks that are not taking the load and require unplanned upgrades.

Value

- Showcase the organization as more collaborative, productive, and competitive.
- Demonstrate that IT has transformed with the cloud and in so doing is appropriately tuned to the organization's present and future needs.
- Reduce workplace stress for IT with the knowledge that there shouldn't be any surprises in terms of performance, scalability, or security, regardless of where the users are gaining access.

LATENCY

Microsoft guidance

Microsoft's own presentation, "**Overcoming Network Performance Blockers for Office 365 Deployments**," at its Ignite conference had this to say about round trip times (RTTs):

- **North America, Mainland NA to NA:** 100-150ms should be the max
- **Europe, Middle East, Africa:** From EMEA site to EMEA data center: < 100ms total should be the aim
- **Asia Pacific:** APAC to EMEA can be done in around 300-320ms as a reference

Further guidance is then offered specifically aimed at **Skype for Business**, where it is noted:

- RTT up to 400ms can be managed
- Exchange in online mode: < 100ms is necessary
- 350ms tends to be the tipping point toward noticeably impaired performance

The bottom line, as presented by Gartner, is that Microsoft broadly recommends the following round-trip latency:

Exchange Online:

Below <50ms for best user experience

Upper threshold is at <275ms

SharePoint Online:

Below <25ms for best user experience

Skype for Business video calls:

Conference or Teams calls with Microsoft-hosted bridge: Do not exceed 100ms

Peer-to-peer calls: Dependent upon end-to-end calling parties

Zscaler™ perspective

Zscaler's goal is to ensure that all end users, regardless of their location, can obtain the first-class user experience that they are after. This effectively means delivering access to Office 365 with < 100ms of true end-to-end latency (wired broadband).

Obviously, it is true that there are multiple elements and data path owners along the way, which is why it is critical to choose each option wisely and why Zscaler data centers are increasingly peered with the Microsoft cloud.

Thanks to this peering, proximity, and full-scale cloud performance, there's simply less complexity/troubleshooting, as well as SLAs that can't be readily achieved with legacy architectures. Even DNS is optimized by Zscaler, as local DNS resolution takes place at each data center, with query times of <1ms.

ROUTING

Microsoft guidance

Microsoft has provided network connectivity guidance on its support page. This article provides very clear recommendations for connectivity/routing:

- A well-configured direct internet connection is the optimal method to connect to Office 365, both in terms of performance and cost.
- Avoid centralized gateways and proxy appliances that can increase latency.
- Leverage local DNS to ensure connections to Microsoft occur in the local region of the client (evaluate cloud proxies if the above isn't possible).
- Avoid network hairpins, which force connections over WANs or VPNs that add intermediate stops or geographical redirections, both of which increase latency.

Zscaler perspective

What appears to be missing from Microsoft's guidance is bandwidth management, as we have seen again and again that it can either make or break the Office 365 user experience. A strategy must exist for managing this experience from every office location, ideally with nearly infinite levels of control.

The reality is that all of this is still largely a hub-and-spoke network, albeit more accurately called hubs-and-spokes in the cloud world, recognizing that the Azure network is now one of your many new hubs to which all locations will now directly route. But it's also about much more than Office 365, as it goes right to the heart of future-proofing the network for additional cloud-based applications to come.

ExpressRoute

“[ExpressRoute for Office365] is very complex and without what we see as typically 2-6 months of planning and work from a large cross skilled team, will very likely result in an outage of your Office 365 implementation.”

—Microsoft

No conversation about Office 365 would be complete without some attention being paid to ExpressRoute. But as we will quickly show, ExpressRoute is only intended to be used by a very small percentage organizations.

Microsoft is abundantly clear on this topic when they say the “cost benefit ratio should be assessed and benefits fully understood,” which is why **Microsoft now has a strict review policy in place before ExpressRoute can be approved for use.**

ExpressRoute can be approved for use

- Good internet connectivity is still required
- A good internet connection may still give similar or better performance
- Often encourages hub-and-spoke model, which may actually increase latency when compared to a direct connection
- Highly skilled network team required
- Higher cost of implementation, usage, and maintenance
- Up to six months of planning required for implementation
- High risk of connectivity problems on cutover if planning and maintenance are not done (e.g., asymmetric routes)
- Security still needs to be applied to the circuit

BANDWIDTH PLANNING

Microsoft guidance

When it comes to planning for the onslaught of Office 365 traffic, Microsoft does offer bandwidth calculators. Keep in mind that your bandwidth requirements can scale quickly as your users embrace the many productivity tools and apps in Office 365. Make sure you set up your network properly from the start, and give yourself plenty of wiggle room in the beginning.

Microsoft's guidance, which is available on the Office 365 support page, suggests the following:

- **Up to 25 users:** Use Excel calculators.
- **Over 25 users:** Start with the calculators as an estimate, then run a pilot and measure the usage during that time.

Zscaler Perspective

The Microsoft view is to measure all the Office traffic you have today, then make your bets on what it will ultimately look like once in the cloud, which is why we have seen organizations, especially the larger ones, run into problems as they move out of their pilot tests and start to scale things up.

Our view at Zscaler is to broadly assume that internet bandwidth consumption may increase by 40 percent, that existing appliance-based firewalls/proxies will ultimately see some level of port exhaustion (more on that later), and that users will quickly wipe out your painstakingly derived estimates.

In the end, customers with their eyes on the cloud don't waste a minute doing such calculations, but rather accept some rational guidance and move forward—provided, of course, that they can truly manage the traffic and prioritize what is most important.

PROXY PLANNING

Microsoft guidance

When it comes to a proxy, Microsoft has the very specific guidance: **it's not recommended**. Detailed through their documentation is the following cautions around running Office 365 traffic through onsite security inspection devices

- **Long lived connections**

Proxies struggle to handle the long-lived connections that Office 365 creates. Apps like Outlook can open up to 20 concurrent connections PER USER. These long-live connections overload appliance hardware and kill performance. In addition, you will quickly run into NAT IP limitations. With 64k ports available per NAT IP address, you'll top out quickly with the number of users you can have behind an IP. Microsoft recommends no more than 2,000 users per NAT IP, but it's best to avoid the challenge altogether.

- **Added Latency**

Proxy and security inspection appliances alter TCP level settings, delay frames, and can add jitter, all which add to the latency of the Office 365 connection.

- **Backhauling**

In today's organization, most proxy and security appliances remain centralized in the gateway. Backhauling Office 365 traffic to a centralized gateway adds insult to injury. In addition to the hardware challenges mentioned above, the connection path itself adds even more latency as it worms its way through your network and security stack.

- **Traffic scaling**

Hardware appliances have limited performance. They are not built with SaaS in mind, which means as your Office 365 traffic grows, you can quickly run into performance limitations.

- **Productivity apps**

Apps like Skype and SharePoint demand the ultimate in low latency. Running these connections through even the best of proxy situations should be avoided.

Zscaler perspective

At this point Microsoft has made it abundantly clear that:

- End-to-end latency must be kept to a minimum at all times;
- Direct internet connections are the recommended approach, both in terms of performance and cost (no ExpressRoute required or even desired); and
- End-to-end bandwidth planning and management is now critically important.

And yet, many will still put aside these clear guidelines, believing that their legacy hub-and-spoke, MPLS-based network that all converges to a single egress point with a large serialized stack of proxy appliances and other bottlenecks will be sufficient, if for no other reasons than it's always worked before and/or it is the easiest path to get connected.

The cloud-rich proxy architecture:

Every single one of the cons related to proxies can be positively addressed by Zscaler. As an example, consider the limit of the 2,000 users per IP, whereas the Zscaler Enforcement Nodes (ZENS), having been built specifically for the cloud, have no 64K port limitations to contend with. And Zscaler Cloud Firewall handles the vast number of long-lived sessions that individual appliance-based firewalls are incapable of, meaning you are free to ramp up the Office 365 user base without any concerns over how many endpoints are going out.

Onboarding Office 365 with Zscaler

Having revealed what Microsoft advises—and backed that up with our own expertise having helped over 700 organizations successfully deploy Office 365—the question now pivots to the advantages Zscaler can offer to your Office 365 network and connectivity. As it turns out, by using Zscaler to deliver Office 365 network connectivity, you get both a fast user experience and a secure direct internet connection, along with key advantages that help simplify administration.

1. ONE-CLICK CONFIGURATION

Most of us in technology prefer to take the easy way when we can. So, it should come as no surprise that those Zscaler customers who are already running Office 365 with great success are big fans of one-click configuration of all the underlying rules.

And what are all of those underlying rules?

Enable Office 365



As Office 365 is a cloud service, its IP addresses are regularly changing, as are its URLs. This happens with such regularity that anyone having to maintain them would be compelled to subscribe to the support RSS feeds from Microsoft and then manually enter those changes. And that's both expensive and no fun for you, which is why we do it as part of our ongoing cloud updates.

Underneath the covers, as the "Enable" option is selected, it simply means that the rules are being auto-updated for you. Of course, if you do prefer to manage it yourself, a quick call to support will allow you take over.

DEPLOYMENT TIP: ESTIMATING O365 ADMINISTRATION

If you are running appliances and backhauling traffic, it's nearly impossible to estimate administrative overhead that Office 365 can add to an IT staff.

One-click configuration highlights why that is true, as a large amount of up-front research and due-diligence would have to take place to determine how many proxies and firewalls would be updated (daily), to say nothing about how they would scale and maintain the low-latency performance needs.

By using one-click to streamline the day-to-day Office 365 administration tasks, your IT team can have time to focus on other IT initiatives and rest assured that optimized connectivity to Office 365 is always up to date.

Onboarding Office 365 with Zscaler

Zscaler peers with Microsoft in major data centers globally. No matter the connection location, the user always gets a local fast connection to Office 365.

2. ROUTE/PEERING OPTIMIZATION

Peering is, without a doubt, one of your best opportunities for taking Office 365 to LAN-like levels of performance.

As part of the standard rollout for any customer who expresses a need or desire for peering, Zscaler works to identify the data centers that are connected to the internet exchanges, which are then directly peered with the Microsoft Azure networks.



And since Zscaler has an open peering policy (meaning we will peer with any provider), this performance may be extended to other key services as well. Once identified and determined to be the best routing option for a customer's given needs, the sites are configured accordingly and the traffic now flows with minimal delay.

And how fast is fast? How about router-to-router roundtrip time (RTT) in < 2ms!

DEPLOYMENT TIP: ROUTING ALL OFFICE 365 TRAFFIC

Even though most associate Office 365 with ports 80 and 443, it is important to understand that the Office 365 application suite uses other non-standard ports. When defining your direct internet connections, you will want to evaluate routing non-standard ports to Zscaler.

Zscaler Cloud Firewall is a great way to help you establish control over your other internet traffic on these direct internet connections.

DEPLOYMENT TIP: GET THE NETWORK RIGHT FROM THE START

It's far better to address internet latency issues before rolling out Office 365. Even if you don't anticipate any issues, or you're just starting out with Word or Excel (not the full Office 365 suite), it's a good idea to know how the traffic will flow once it hits your internet circuits, rather than guessing or crossing your fingers.

In addition, as your users embrace Office 365 and its productivity advantages, your small installation can escalate quickly. Apps like Skype, SharePoint, and Teams are enticing to users, but they require a well-thought out direct-to-cloud network.

It is best to make sure your network can handle the latency of all apps available in the suite up front, so once the Office 365 train leaves the station, you're prepared.

Onboarding Office 365 with Zscaler

3. BANDWIDTH CONTROL

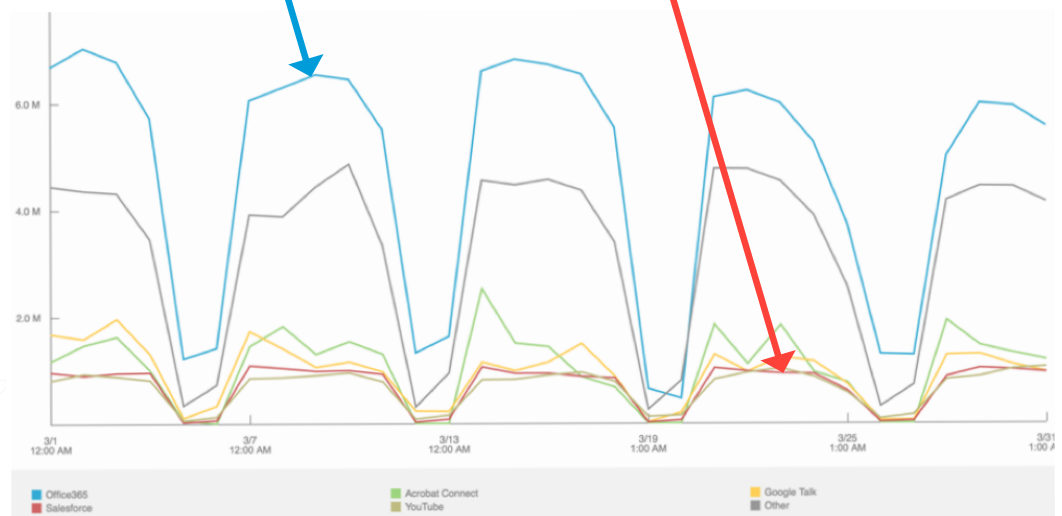
If it's not already obvious, the network for Office 365, like every other cloud-based application, is the internet, not the corporate LAN or WAN. This is precisely why we all increasingly see articles saying that the corporate network, just like the corporate data center, is largely going away. And as it relates to security, if you don't control the network, you can't have network security. But the reality for Office 365 is that the network is where the transformation is primarily focused, which is precisely why it demands so much renewed attention.

So the question becomes: how do you manage the traffic once it leaves your perimeter router?

And the answer is: through the use of Zscaler Bandwidth Control and ensuring that every packet going to Office 365 has the absolute shortest path, with little to no latency before it hits the internet connection.

40% of bandwidth is reserved for Office 365 during periods of contention.

During these times, YouTube is **capped at 20%.**



DEPLOYMENT TIP: REMEMBER TO PRIORITIZE

No large organization will be able to properly scale Office 365 without addressing app prioritization with bandwidth control.

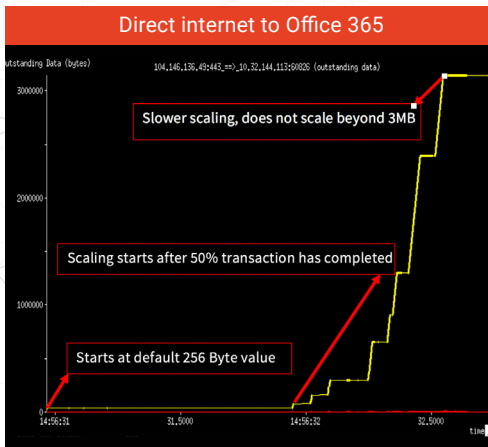
By acknowledging this need ahead of time and ensuring that IT efficiency is designed in, any organization can forego the inevitable demand for excessive increases in bandwidth or any of the potential bottlenecks along the way.

You can see in the example above how Zscaler Bandwidth Control enables Office 365 traffic to be prioritized over YouTube.

Onboarding Office 365 with Zscaler

4. UNDER THE COVERS: OPTIMIZATIONS

When we dive deeper into the global Zscaler cloud platform, we can see how performance is directly optimized around Office 365 connectivity. The TCP/IP graphs to the left highlight how connections typically occur to Office 365 cloud endpoints, and how Zscaler addresses connections as they're routed through its cloud platform.

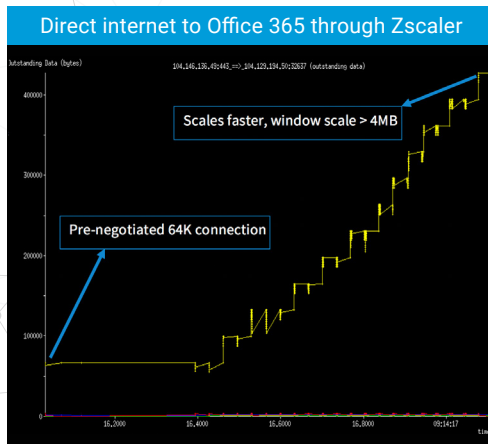


Direct internet to Office 365

In this simple file download transaction, you can see how the TCP connection scaling is handled. Notice how communication must start at a default value and really only starts to scale after the transaction is 50 percent completed? Then, above a certain point, scaling doesn't improve.

Direct internet to Office 365 through Zscaler

When downloading the same file through the Zscaler cloud platform, you can see right off the bat you get a pre-negotiated robust 64K byte connection, far above the default 256 byte connection shown above. Then, as soon as the data transfer starts, it ramps up as you would expect it to, allowing it to scale much faster and well beyond the 3MB limit imposed before.



Under the covers, Zscaler is doing some key adjustments to TCP/IP, such as:

- **Forcing a large TCP window size** per connection, with a flexible receive buffer that makes large file downloads faster.
- **Disabling the Nagel algorithm** to facilitate higher performance for all those long-lived Office 365 connections.
- **Setting a flexible TCP idle timeout** at 120sec, further keeping the connections alive on the user's behalf.

NEXT STEP

To learn more about how Zscaler can enable your Office 365 deployment with a fast user experience, download the Zscaler for [Office 365 Solution Brief](#).

ABOUT ZSCALER

Zscaler enables the world's leading organizations to securely transform their networks and applications for a mobile and cloud-first world. Its flagship services, Zscaler Internet Access™ and Zscaler Private Access™, create fast, secure connections between users and applications, regardless of device, location, or network. Zscaler services are 100% cloud delivered and offer the simplicity, enhanced security, and improved user experience that traditional appliances or hybrid solutions are unable to match. Used in more than 185 countries, Zscaler operates a multi-tenant, distributed cloud security platform that protects thousands of customers from cyberattacks and data loss. Learn more at [zscaler.com](https://www.zscaler.com) or follow us on Twitter [@zscaler](https://twitter.com/zscaler).

