WHITE PAPER

The Definitive Guide to Networking for Office 365

Is it possible to implement an Office 365-ready network, at scale, without a proof-of-concept (PoC)? Your CIO has tapped you to lead the effort to move to Office 365. Realizing it's a great opportunity and distinction in your career, you reply with, "Sure, I'll make sure it is a total success!" and then note that a PoC will not be needed. Bold move...and here's why:

First, let's consider the following:

- The CIO (and more often than not the business itself) has likely already made up his/her/their mind that the future is, without a doubt, running Office 365.
- Office 365 is not a concept—it works! It also doesn't need to be proven to scale—it scales just fine, as has been proven in many very large organizations.
- If the project fails to scale for your organization, you can bet the blame won't fall to Microsoft or the company executives who selected it, but rather to the implementer's ability to achieve success in the environment. And isn't this always how it goes?

This is the world we now live in, where the business is selecting the cloud platforms to carry them forward and IT is not so much a part of that selection process, but rather a blunt, albeit highly skilled, instrument of implementation and support. It's commodity IT services at its best, where the transformational leaders are rising to the challenge and playing by the new set of rules.

So now back to the question of whether or not it's possible, even advisable, to press forward with the deployment without IT first having a trial run at it? The answer to that is it's not only possible, but it might very well be one of the best experiences you have ever had in your career. But getting there means following the advice of those who have gone before, adhering to their wisdom via best practices documentation and recommendations from Microsoft.

The intent of this guide it to 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, you might very well come to the conclusion that you can accelerate the future while also saving your organization more time and money than would otherwise have been anticipated.

700+
Customers on Office 365

1.8 PB
Office 365 traffic per month and growing

131 TB
Monthly Office 365 traffic from one customer alone

As we begin, let's first consider our objectives, metrics, and values as they specifically relate to the network and/or security. In a sense, this would be your contract with the organization for your end of the services you provide in getting them to a better place.

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, outwardly recognized by customers and partners as skilled leaders in this area of excellence.

Metrics

- Certify that 100% of staff are fully familiarized with all relevant best practice deployment standards and documentation.
- Validate that < 30ms of latency is achievable from all locations, including branch offices, at all times with respect to any and all Office 365 traffic.
- Provide clear evidence that we deployed faster and with better results than at least two previous organizations of similar size and complexity.
- Validate that there are no (zero) "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 competitive.
- Earn praise and acknowledgment from the organization that IT, itself, has transformed with the cloud and in so doing is appropriately tuned to the present and future needs.
- Reduced workplace stress, as IT is able to sleep well at night, knowing that there should be no surprises in terms of performance, scalability, or security, regardless of where the users are gaining access.
- Retain great employees (across the company), as they will be impressed by running fresh and high-performance tools that allow them to better meet their own personal and professional goals.

Problem: Organizations the world over continue to leverage network and security architectures that were never designed for the larger cloud applications, resulting in all-too-often embarrassing situations for IT leadership as they struggle to provide a LAN-like experience to cloud applications. Gartner highlighted this issue in its August 2016 report on Office 365: "Existing internet connectivity to Office 365 will not be 'good enough' for most Office 365 usage scenarios."

Solution: Taking these definitive best practices seriously, any organization can achieve great success not only with Office 365, but with other large-scale cloud applications as well. After all, these guidelines represent the very best insight and wisdom from not only Microsoft (with the Azure network as one of the top three networks in the world), but also Zscaler (with hundreds of successful Office 365 deployments).

LATENCY

Microsoft Guidance

Microsoft's own presentation **"Overcoming Network Performance Blockers for Office 365 Deployments"** at its 2016 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<> 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 tend to be the tipping point toward noticeably impaired performance

The bottom line, as presented by Gartner, is that Microsoft broadly recommends round-trip latency of <275ms, <50ms for Exchange Online, and <25ms for SharePoint Online.

Of course all of this is with the full recognition that there are multiple elements in play, including:

- Client to Customer Egress (Customer Managed)
- Egress to Microsoft Network Edge (ISP or Customer Managed)
- Microsoft Network Edge to Office 365 Endpoint (Microsoft Managed)

Zscaler's Expert View

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's 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 released additional **Office 365 connectivity guidance** via their TechNet blog series "On The Wire". This blog provides very clear recommendations for connectivity/routing, whereby Microsoft offers the following guidance.

- A well-configured, direct internet connection is the optimal method to connect to Office 365, both in terms of performance and cost.
- Avoid centralized proxies which can increase latency.
- Ensure they are in the local region of the client (evaluate cloud proxies if the above isn't possible).
- WAN optimization is not a supported use case.

Zscaler's Expert View

What appears to be missing from Microsoft's guidance is bandwidth management, as we have see time and time again that it will either make or break the Office 365 user experience. Without this level of detail, latency will be far out of tolerance, as will the business temperament itself. A strategy must exist for managing this experience from every office location, ideally with virtually 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

No conversation about Office 365 would be complete without some attention being paid to ExpressRoute. But as we will quickly show, it's really only intended to be used by a very small percentage of organizations. Consider Microsoft's clear position on where this fits.

Microsoft is abundantly clear and certainly deliberate 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 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*

Challenges with ExpressRoute – Directly from Microsoft

- 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

Microsoft offers the following guidance when it comes to bandwidth planning for Office 365:

- **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's Expert View

Zscaler's view of bandwidth management is quite different from Microsoft's, which clearly isn't well defined at the moment.

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 really start to scale things up.

Our view at Zscaler is to broadly assume that internet bandwidth consumption might 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. Because those who can't are really left with no options other than following Microsoft's rather defensive position of forcing you to fully calculate everything on your own, or just accepting the risk of partial or even complete failure.

PROXY PLANNING

Microsoft Guidance

Finally, if/when a proxy must be used:

- Ensure the devices are scaled up to cope with SaaS services, both in terms of processing and NAT capability.
- Avoid centralized proxies which can increase latency.
- Ensure proxies, are in the local region of the client.
- Ensure all setting are checked and optimized.
- Avoid using Skype for Business through these devices, even when optimized.
- Avoid unnecessary packet inspection.
- Evaluate cloud proxies if the above isn't possible.

Microsoft then goes on, articulating its own list of cons for **cloud poor** proxy architectures:

- Proxies generally do not handle UDP traffic; therefore Skype traffic is forced over TCP, resulting in Skype's coping mechanism for poor networks kicking in.
- Proxies can delay frames on their way through, adding jitter and latency which is hard to identify.
- Older proxies often struggle to deal with the long-lived, high-throughput connections SaaS services entail.
- Proxies alter TCP level settings, which can cause performance issues.
- SSL issues can also occur as the proxy is the "man in the middle."
- Proxies often don't scale and were not installed/ designed with SaaS services in mind, resulting in poor quality and performance.
- There should be no more than 2,000 users behind each NAT'd public IP address. This is because Office 365 client applications can routinely open between 12-20+ connections per device, and there are NAT limitations due to only having 64K ports per IP. You can perhaps stretch this a bit, but only if you are willing to do some exhaustive assessments and calculations.

Zscaler's Expert View

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);
- 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 user per IP, whereby the Zscaler Enforcement Nodes (ZENs), having been built specifically for the cloud, have no 64K port limitations to contend with. And the cloud firewalls best handle the vast number of long-lived sessions than individual appliance-based firewalls are capable 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

HOURS VS. [DAYS-WEEKS-MONTHS]

Having revealed what Microsoft advises—and backed that up with our own expertise with over 700 Office 365-enabled customers to our credit—the question now pivots to what the enablement actually looks like. Who does what...and why?

As it turns out, the process is really simple from here on in, provided, of course, that Microsoft's clear and compelling guidelines have been followed. The flick of a switch, perhaps some route optimizations, and then some bandwidth management is really all that remains, at least as far as the network is concerned.

And then...proof. The proof that Office 365 can excel in the way Microsoft intended and that the Zscaler-optimized network ensures it does.

1. CLICK TO ENABLE

Most of us in technology prefer to take the easy way when we can. Sure, there are those who prefer to do all the math and calculate every move, but they are clearly in the minority. So, it should really come as no surprise that those Zscaler customers who are already running Office 365 with great success are big fans of one-click enablement of all the underlying rules.

And what are all of those underlying rules?

Well, 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.

PoC Avoidance

If you are running appliances and backhauling traffic, there's virtually no way to get around a proof-of-concept, or at least a rather exhaustive pilot.

This button 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.

If you believe that true wealth is the discretionary free time that allows you to take on other endeavors, then having to dig into and maintain the great minutia of rules for a critical service is the clearly opposite of where you want to go.

2. ROUTE/PEERING OPTIMIZATION

Peering is, without a doubt, one of the best opportunities available 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 round trip time (RTT) in < 2ms!

ROUTING ALL OFFICE 365 TRAFFIC

Even though most associate Office 365 with ports 80 and 443, it is important to understand that Office 365 uses other non-standard ports. When defining your direct internet connections, be sure to route all your traffic to Microsoft.

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

PoC Avoidance

It's far better to address internet latency issues before rolling out Office 365. Even if you don't anticipate any issues, it's a good idea to know how the traffic will flow once it hits your internet circuits, rather than guessing or hoping that all is well.

To put it another way, it simply doesn't make sense to design and conduct a PoC exercise when the need is clearly identified and can be addressed without the extra effort.

While some may try to leverage a PoC to point out gaps with the network architecture or readiness thereof, it's a more professional move to acknowledge that this can be addressed up front at far less cost and effort by thoughtful design and quality consultation. And if any outside consultant isn't knowledgeable about the value of cloud proxies, then it's questionable whether the consultant really knows Office 365 networking.

3. BANDWIDTH MANAGEMENT

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 and thought leadership.

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's bandwidth management 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.

PoC Avoidance

No large organization will be able to properly scale Office 365 without addressing bandwidth management. Eventually this will come to light as there will, of course, be a test.

Here again, a PoC exercise is not really needed. By simply acknowledging the need ahead of time and ensuring that IT efficiency is designed in, any organization can forego the inevitable late-breaking (reactionary) decisions for excessive increases in bandwidth or any of the potential bottlenecks along the way.

Since all of this has already been learned ahead of time, there's simply no need for anyone else to have to learn the hard way all over again.

You can see in the example below just how Office 365 traffic is being prioritized over YouTube. Zscaler also boasts a single customer doing full bandwidth management for 1.6 million users, so it's clear that this is, itself, not a simply concept.

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

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

CAN YOU PROVE IT PERFORMS?

ABSOLUTELY - AND THEN SOME

All the theory and proclamations mean very little if the results aren't truly verifiable. And by truly verifiable, we of course mean what you and the users can see and feel for yourselves on a daily basis, but also what can be proven by third-party verification.

This is why Zscaler relies on Catchpoint as a trusted third-party web performance monitoring service. Catchpoint is uniquely capable of measuring just how well the Zscaler architecture performs, and specifically how it performs for key cloud services such as Office 365.

We pulled live data, just as seen every minute of every day across the Zscaler cloud, to show, exactly and without any fluff, what performance benefits can be seen in North America, Europe, and Asia/Pacific.

TO REVIEW THE FULL TEST RESULTS, YOU CAN DOWNLOAD THE CATCHPOINT REPORT FROM HERE:

https://www.zscaler.com/resources/industry-reports/catchpoint-office-365-benchmark-report.pdf

Here's a clear comparison of files downloaded directly and through three Zscaler data centers. This data is for a 3MB file, hosted on a SharePoint site in the U.S., and using local ISPs for the corporate internet connectivity. You will notice remarkable gains in the time to download, resulting in the user getting the file much faster going through Zscaler than going direct! This is not a photo finish, but rather a performance boost that the users themselves can see and feel.

File download times

Zscaler file download times were faster than going direct. The fastest Zscaler download time was 1 second in Chicago; the fastest direct download was 2 seconds. The average download time for Zscaler was 2.5 seconds and 4.2 seconds for direct. Chennai had the longest download times with 4.6 seconds for Zscaler and 8.6 seconds for direct. See figure 1.

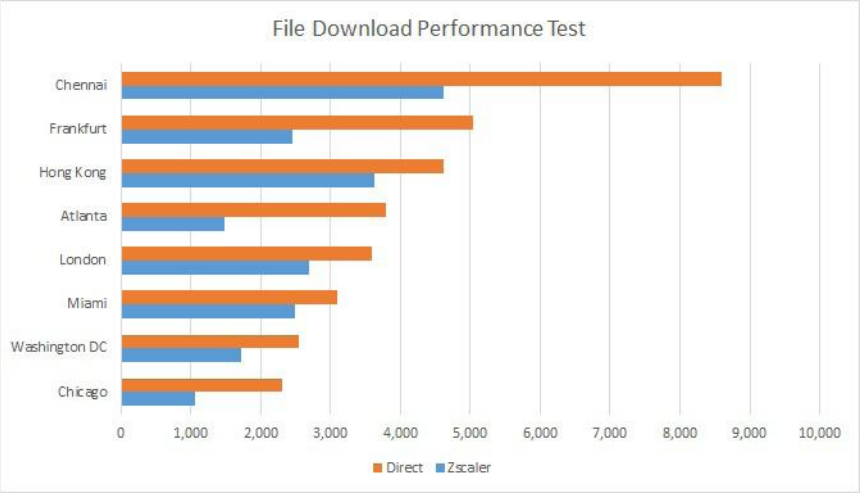


Figure 1

DNS connection times

In every test, Zscaler DNS connection times were significantly faster than going direct. In some tests, connection time for Zscaler were less than 1 ms. DNS connection times for direct were as high as 346 ms, with an average of 170 ms. See figure 2.

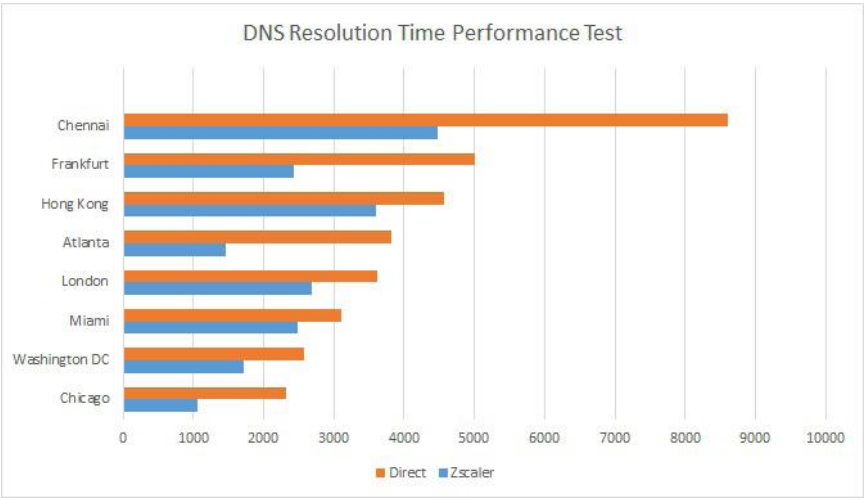
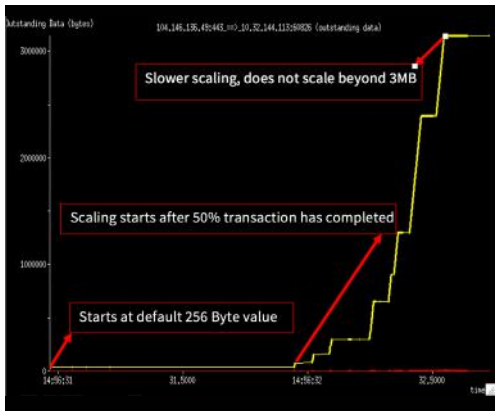


Figure 2

When we go much deeper into the transaction, really focusing on what is going on with TCP/IP, we can see where Zscaler picks up the performance.

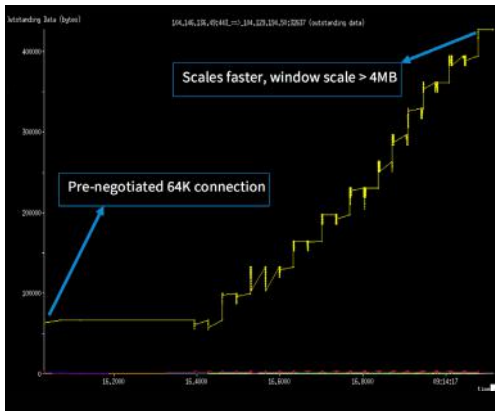


Direct (not going through Zscaler)

This is simply the transaction setup without the benefit of the Zscaler cloud. Notice how IP communication must start at a default value and really only starts to scale after the transaction is 50% completed? Then above a certain point, scaling doesn't improve.

Zscaler Route

Here, the Zscaler Enforcement Node (ZEN) has pre-negotiated a 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 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 STEPS

To learn more about the Office 365 and Zscaler performance testing presented in this document, download the **CatchPoint Performance Report**

To learn more about Zscaler for Office 365, see the **Solution Brief**

ABOUT ZSCALER

Zscaler services enable customers to move securely to a modern cloud architecture. The Zscaler cloud connects users to applications, regardless of where users connect or where the applications are hosted, while providing comprehensive security and a fast user experience. Zscaler offers two service suites that eliminate the cost and complexity of gateway appliances. Zscaler Internet Access securely connects users to internet and SaaS applications, scanning every byte of traffic to protect against cyber threats and data leakage. Zscaler Private Access provides fast access to internal applications hosted in the data center or public clouds—without a VPN. Used in more than 185 countries, Zscaler protects thousands of enterprises and government agencies from cyberattacks and data loss. Learn more at **www.zscaler.com**.

CONTACT US

Zscaler, Inc.
110 Rose Orchard Way
San Jose, CA 95134, USA
+1 408.533.0288
+1 866.902.7811

www.zscaler.com

FOLLOW US

facebook.com/zscaler
linkedin.com/company/zscaler
twitter.com/zscaler
youtube.com/zscaler
blog.zscaler.com

softwerx

zscaler™