catchpoint™

CONNECTIVITY OPTIONS FOR MICROSOFT OFFICE 365

Evaluate deployment options and performance through independent testing

Microsoft Office 365 is the latest in the long list of enterprise applications to leave the confines of the corporate-controlled data center for the cloud. As enterprises rely more and more on cloud applications to run their businesses, they face challenges imposed by traditional hub-and-spoke architectures.

When Microsoft Exchange servers and Office applications were on-premises, you had to backhaul traffic from remote sites and mobile users to the data center. It was the only way to provide connectivity. But now that these services have moved to the cloud in the form of Office 365, backhauling all your traffic to your data centers introduces a lot of complexity that can impact performance and quickly lead to frustrated users and delayed deployments.

Acknowledging these issues, at the Microsoft Ignite Conference in September 2016, Microsoft introduced new guidance on best practices for enterprises looking to deploy Office 365.

Summary of Best Practices for a successful Office 365 deployment – Ignite, 2016

- Direct Internet connections are the optimal method in terms of performance and cost.
- Hub-and-spoke architectures with centralized proxies should be avoided as they introduce latency and proxies struggle to deal with long-lived sessions and high-throughput connections.
- Express Route should only be used in a small number of use cases as it's highly complex to configure correctly.

Why Office 365 presents challenges for legacy networks

The use of Office 365 in the enterprise can create a significant increase in network utilization, because each Office 365 user will generate between 12 and 20 persistent connections. This increase can easily overwhelm firewalls and increase transport costs. To mitigate these issues, Microsoft has issued new recommendations for organizations deploying Office 365 on hub-and-spoke architectures with centralized proxies, including performing NGFW capacity assessments and WAN latency assessments. Furthermore, Microsoft now advises against using Skype for business when deploying Office 365 on such networks.

Microsoft's support documentation would seem to echo its concerns about Office 365 performance on hub-and-spoke networks. In these guidelines, Microsoft states that Office 365 was built to be accessed securely and reliably via a direct Internet connection. Microsoft further notes that it has invested heavily in a content-delivery network (CDN) to accelerate the delivery of content to users and, thus, wants users to connect to their network as fast as possible.

support.office.com/en-us/article/Azure-ExpressRoute-for-Office-365-6d2534a2-c19c-4a99-be5e-33a0cee5d3bd

Direct-to-Internet deployment options for Office 365

With direct-to-Internet determined to be the best way to access Office 365, we set out to evaluate which direct approach would be best for the organization.

The first deployment option we considered was to use next-gen firewalls or UTMs to route Office 365 traffic locally to the Internet. While this approach eliminates any latency concerns of backhauling traffic, it requires appliances at every branch location. If you have a lot of branches, such a deployment would quickly become prohibitively expensive and introduce a lot of administrative overhead. Microsoft warns that Office 365 requires constant firewall updates, and that missing an IP or URL update will result in end-user connectivity problems. This deployment option also leaves out mobile users, requiring them to use VPN for Office 365 access, which needs to be considered when assessing the user experience.

The second deployment option we decided to investigate was the use of cloud-delivered security. In this case, we partnered with Zscaler to understand how the Zscaler Cloud Security Platform could be used to route Office 365 and Internet traffic locally. With Zscaler there was no hardware to deploy, so getting started only required some basic routing changes to forward traffic to the closest Zscaler data center. The Zscaler platform includes a Cloud Firewall, with full next-gen capabilities, so traffic isn't limited to ports 80 and 443. One of the benefits of using the Zscaler Cloud Firewall is that it simplifies administration by making Office 365 setup a checkbox.

Evaluating Zscaler

Zscaler states that it has over 700 successful Office 365 deployments to date and is processing over 1.2 petabytes of Office 365 traffic per month. In addition to peering with Microsoft in major data centers, the company claims to offer several performance advantages, including fast and local DNS, window scaling for faster file downloads, and the ability to prioritize Office 365 traffic over other Internet traffic.

Performance testing

To better understand the user experience when going direct-to-Internet for Office 365, we decided to run a series of file download tests in eight cities around the world.

1. Atlanta
2. Chennai
3. Chicago
4. Frankfurt
5. Hong Kong
6. London
7. Miami
8. Washington, DC

Methodology

The tests consisted of clicking on a URL that would download a 2MB WebEx Player hosted on SharePoint. Each location was configured to perform two tests: one used a direct connection and one went through the Zscaler Cloud Security Platform. For direct tests, the request was made simply by clicking on the file URL. For Zscaler tests, the request was routed through the closest Zscaler data center. The tests were set to run automatically every 15 minutes over three days using Synthetic Monitoring, which simulates the exact user behavior to download the file.

In each test, we recorded the DNS resolution, file download times, and geometric mean was used to determine the user experience.

- DNS resolution: The amount of time it took to resolve the domain name of the host
- File download: The amount of time it took to download the entire 2MB file (WebEx player)

PERFORMANCE TEST FINDINGS

File download times

Zscaler file download times were 40 percent 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.

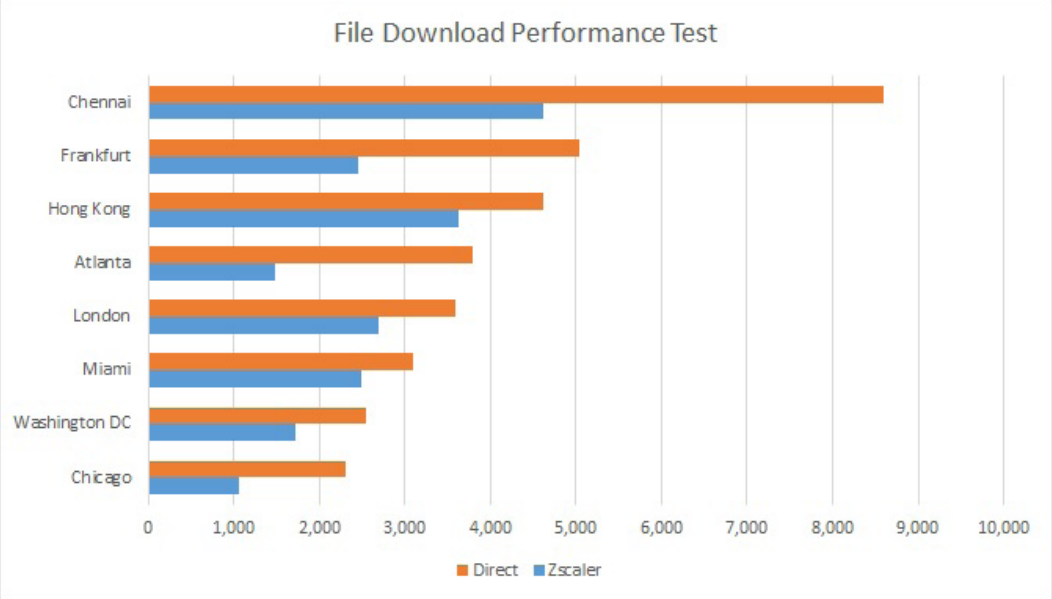

Figure 1

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.

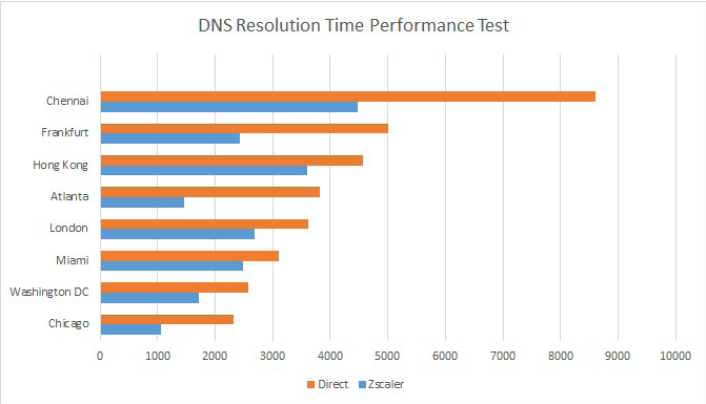

Figure 2

Conclusion

The migration to Microsoft Office 365 is well under way, with most enterprises having already made the decision to begin the process. In light of Microsoft's latest guidance for deployment, enterprises need to adapt their current hub-and-spoke architectures and route Office 365 traffic locally to the Internet.

In this report we investigated two approaches for routing traffic locally – going direct and using the Zscaler Cloud Security Platform – and the impact they had on the user experience. After all, it's the user experience that will determine whether or not the move to Office 365 will be considered a success.

In the tests conducted by Catchpoint, Zscaler provided the best Office 365 user experience with the fastest download speeds. We attribute the performance advantage to the TCP optimization enabled by Zscaler, its fast-local DNS and TCP times, and its direct peering with Microsoft Office 365.

As you evaluate your options for deploying Microsoft Office 365, we highly recommend using the Zscaler Cloud Security Platform.

About Catchpoint

Catchpoint Systems is a leading Digital Performance Analytics company. Designed for digital business, Catchpoint is the only end-user experience monitoring (EUM) platform that can simultaneously capture, index, and analyze object-level performance data inline.