# Table of Contents

## Introduction ......................................................................................................................... 3

## The Topic of VPN .................................................................................................................. 4
   - Secure Internet traffic and enable DLP policies ................................................................. 4
   - Allow IT to provide support to endpoints and remote patching ...................................... 5
   - Do's and Don'ts ................................................................................................................. 5

## Quick Implementation Guide for Office 365 Optimisation .................................................. 6

## Common questions when implementing local breakout and split tunnelling for Office 365 ................................................................................................................................. 9
   - How do I stop users accessing other tenants I do not trust where they could exfiltrate data? ................................................................................................................................. 9
   - Does this model allow access to consumer services such as personal OneDrive accounts? ................................................................................................................................. 9
   - How do I apply DLP and protect my sensitive data when the traffic no longer flows through my on-premises solution? ................................................................. 9
   - How do I evaluate and maintain control of the user's authentication when they are connecting directly? ................................................................. 10
   - How do I protect against viruses and malware? ................................................................ 10
   - Can I send more than just the Optimize traffic direct? ......................................................... 10
   - Why is port 80 required? Is traffic sent in the clear? ............................................................ 10
   - Does this advice apply to users in China using a worldwide instance of Office 365? ........ 11

## Quick Implementation Guide for Cisco Webex Meetings ..................................................... 12
   - List of IP address ranges used by Cisco Webex Meeting services ...................................... 12
   - List of Domains used by Cisco Webex Meeting Services ..................................................... 12
   - List of Domains used by Webex Teams .............................................................................. 12

## Quick Implementation Guide for Zoom ............................................................................... 14
   - List of IP address ranges used by Zoom ............................................................................ 14
   - List of IP address ranges used by Zoom Phone ................................................................. 15
   - List of Domains used by Zoom .......................................................................................... 15

## Training your Users ............................................................................................................. 16
   - How to check the connection quality ................................................................................ 17
Introduction

Many organisations haven’t experienced a high rate of remote workers such as what’s happening during the outbreak of COVID-19 throughout the world.

While most networks are able to cope with an average load, when this load doubles or triples compared to the norm, bottlenecks will become evident and the experience degrades for your users.

Are your key digital resources accessible easily from outside the office? Is the experience maintained when doing so? What about security? If you built your security around the corporate perimeter, you may find this new way of working leaves sensitive data exposed.

This white paper will guide you through some of the key topics to address, and give you quick, actionable guidance to improve how your network and infrastructure is configured, to maximise the experience while maintaining security end-to-end for your users and data.
The Topic of VPN

While there is a lot of ground to cover on how to mitigate the impact on your organisation during these testing times, VPN usually deserves the first spot.

Usually there are a few reasons for which businesses deploy VPNs:

- Allow access to on-premises applications when remote
- Secure internet traffic and enable DLP policies
- Allow IT to provide support to endpoints and remote patching

How to get around these issues and solve them in an effective way while offloading as much burden as possible from your corporate appliances and network egresses?

Allow access to on-premises applications when remote

- Migrate all possible workloads to cloud-native solutions that don't run in your network. An obvious example is to move email to Exchange Online, Skype for Business on-premises to Microsoft Teams, legacy HR suites to Workday or SuccessFactors.

- For applications that can't or won't be migrated anytime soon, publish them on the internet and protect them with Azure AD Application Proxy. With a bit of work to implement it at the app level if developed in-house, it's possible to easily pass through the authentication to your app. If not, App Proxy will add an additional layer of authentication, including MFA and Conditional Access policies, in front of your application, without touching the code, and more importantly, not requiring VPN.

Secure Internet traffic and enable DLP policies

- Rather than centralise this function using your corporate firewalls and proxy solutions, consider deploying it client-side. Solutions such as Zscaler Internet Access or Cisco Umbrella move the security from the 'hub-and-spoke' model, directly to the endpoints, with a service delivered straight from their cloud.
Allow IT to provide support to endpoints and remote patching

- Consider migrating from a classic SCCM deployment, to a hybrid management with Intune, where all machines can connect directly to cloud for their patching and configuration needs. This will reduce the dependency on VPNs.

Do's and Don'ts

- Do deploy split tunnelling and make sure NOT to tunnel any cloud applications, especially those related to realtime communication, as double encryption over unsuitable transports such as TCP instead of UDP, will result in very bad experience and high load on the VPN appliances.
- Do provide access to LoB apps by using Azure AD Application Proxy.
- Don't deploy always-on VPN solutions, try to minimise the need for users to even have to use VPN in the first place.
- Don't deploy full tunnelling without caring about the workloads that will cross said tunnel.
- Don't make all cloud applications cross a web proxy once connected to the VPN, especially those that leverage realtime media, as proxies are not suitable and/or supported by most cloud applications such as Office 365, and will result in a poor experience for the users.
- Do deploy Microsoft Azure Traffic Manager to geolocate VPN users. This allows you to send users to their nearest gateway automatically and to meet scale demands.
- If possible, do use a dynamic and scalable authentication mechanism like Azure Active Directory, to avoid the trouble of certificates and improve security using multi-factor authentication (MFA) if your VPN client is Active Directory aware. One such example is the Azure OpenVPN Client.
Quick Implementation Guide for Office 365 Optimisation

This below is how lots of company networks were traditionally configured. With remote workers all connecting back to HQ via VPN and then egressing the network through the on-premises infrastructure, funnelling all traffic through the VPN appliances and the centralised WAN.

This approach doesn’t work well in the era of cloud services and distributed workforces.

As mentioned above, the solution is to split the cloud-sensitive traffic from the rest. Here’s how to do it:

You will need to enable optimised access to a list of endpoints which are Microsoft-Owned and follow these characteristics:

- Are Microsoft owned and managed endpoints hosted on Microsoft infrastructure.
- Have IPs provided
- Low rate of change to URLs/IPs compare to other two categories
- Expected to remain low in number of URLs
- Are High volume and/or latency sensitive
<table>
<thead>
<tr>
<th>Endpoint to Optimise</th>
<th>Port/s</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="https://outlook.office365.com">https://outlook.office365.com</a></td>
<td>TCP 443</td>
<td>This is one of the Core URLs Outlook uses to connect to its Exchange Online server and has high volume of bandwidth usage and connection count. Low network latency is required for online features including: Instant search, Other mailbox calendars, Free / busy lookup, manage rules &amp; alerts, Exchange online archive, Emails departing the outbox.</td>
</tr>
<tr>
<td><a href="https://outlook.office365.com">https://outlook.office365.com</a></td>
<td>TCP 443</td>
<td>This is use for Outlook Online web access to connect to its Exchange Online server and network latency. Connectivity is particularly required for large file upload and download with SharePoint Online.</td>
</tr>
<tr>
<td>https://&lt;tenant&gt;.sharepoint.com</td>
<td>TCP 443</td>
<td>This is the primary URL for SharePoint Online and has high volume of bandwidth usage.</td>
</tr>
<tr>
<td>https://&lt;tenant&gt;-my.sharepoint.com</td>
<td>TCP 443</td>
<td>This is the primary URL for OneDrive for Business and has high volume of bandwidth and possibly high connection count from the OneDrive for Business Sync tool.</td>
</tr>
<tr>
<td>Teams Media IPs (no URL)</td>
<td>UDP 3478, 3479, 3480 and 3481</td>
<td>Relay Discovery allocation and real time traffic (3478), Audio (3479), Video (3480), and Video Screen Sharing (3481). These are the endpoints used for Skype for Business and Microsoft Teams Media traffic (Calls, meetings etc). Most endpoints are provided when the Microsoft Teams client establishes a call (and are contained within the required IPs listed for the service). UDP is required for optimal media quality.</td>
</tr>
</tbody>
</table>

<tenant> should be replaced with your Office 365 tenant name. For example contoso.onmicrosoft.com would use contoso.sharepoint.com and contoso-my.sharepoint.com

At the time of writing (Mar 2020), the IP ranges which these endpoints correspond to are as follows. It is strongly advised to check the URL/IP page to check for any updates when applying the policy, and do so on a regular basis.

It’s worth noting that Microsoft also makes available a [REST API Web Service](#) that provides the up to date IPs and a [PowerShell Example Script](#) that queries it and outputs the URLs/IPs/Ports for all relevant IP categories.

<table>
<thead>
<tr>
<th>IP Range</th>
<th>IP Range</th>
<th>IP Range</th>
<th>IP Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>104.146.128.0/17</td>
<td>13.107.128.0/22</td>
<td>13.107.136.0/22</td>
<td>13.107.18.10/31</td>
</tr>
<tr>
<td>13.107.6.152/31</td>
<td>13.107.64.0/18</td>
<td>131.253.33.215/32</td>
<td>132.245.0.0/16</td>
</tr>
<tr>
<td>150.171.32.0/22</td>
<td>150.171.40.0/22</td>
<td>191.234.140.0/22</td>
<td>204.79.197.215/32</td>
</tr>
<tr>
<td>23.103.160.0/20</td>
<td>40.104.0.0/15</td>
<td>40.108.128.0/17</td>
<td>40.96.0.0/13</td>
</tr>
</tbody>
</table>
IPV6 endpoints can be ignored if not currently required, i.e. the service will currently operate successfully on IPV4 only (but not the other way round). This will likely change in future but IPV4 only is possible for the time being.

Now that we have identified these critical endpoints, we need to divert them away from the VPN tunnel and allow them to use the user’s internet connection to connect directly to the service. The vast majority of VPN solutions allow split tunnelling, where identified traffic is not sent down the VPN tunnel to the corporate network but rather sent direct out the user’s local internet connection. The VPN client should be configured so that traffic to the above, Optimize marked URLs/IPs/Ports are routed in this way. This allows the traffic to utilize local Microsoft resources such as Office 365 Service Front Doors such as AFD as one example, which deliver Office 365 services & connectivity points as close to your users as possible. This allows us to deliver extremely high performance levels to users wherever they are in the world. There is also Microsoft’s world class global network which is very likely within a small number of milliseconds of your users direct egress, and is designed to take your traffic securely to Microsoft resources wherever they may be in the world, as efficiently as possible.

The solution would look something like that below:

Split Tunnel VPN solution

Sounds simple? It is in most cases, but for an enterprise, this shift in connectivity invariably raises questions about security. In the traditional network approach security is often applied inline to network traffic as it egresses to the internet. Proxies and firewalls perform inspection on the traffic to check for data exfiltration, viruses and so on. By bypassing this we are removing this layer of protection we have come to rely on when connecting to the internet. The good news is, for the highlighted endpoints above, Microsoft has numerous features in place which means your security with the modern approach may well be higher than available previously.
Common questions when implementing local breakout and split tunnelling for Office 365

It should be noted that the two steps above are all that is necessary to solve the performance/scalability issues if you need to move very quickly given the current situation. The elements below can be added as needed and as time allows or you may have them in place already.

How do I stop users accessing other tenants I do not trust where they could exfiltrate data?

The answer is a feature called tenant restrictions. Authentication traffic is not high volume nor especially latency sensitive so can be sent through the VPN solution to the on-premises proxy where the feature is applied. An allow list of trusted tenants is maintained here and if the client attempts to obtain a token to a tenant which is not trusted, the proxy simply denies the request. If the tenant is trusted, then a token is accessible if the user has the right credentials and rights.

So even though a user can make a TCP/UDP connection to the Optimize marked endpoints above, without a valid token to access the tenant in question, they simply cannot login and access/move any data.

Does this model allow access to consumer services such as personal OneDrive accounts?

No, it does not, the Office 365 endpoints are not the same as the consumer services (Onedrive.live.com as an example) so the split tunnel will not allow a user to directly access consumer services. Traffic to consumer endpoints will continue to use the VPN tunnel and existing policies will continue to apply.

How do I apply DLP and protect my sensitive data when the traffic no longer flows through my on-premises solution?

If required, endpoints can be protected with Office DLP if required and it's much more efficient to provide this feature in the service itself rather than try and do it in line at the network edge. Azure Information protection can also be used to provide a high level of information protection if required.
How do I evaluate and maintain control of the user’s authentication when they are connecting directly?

In addition to the tenant restrictions feature noted in question 1, conditional access policies can be applied to dynamically assess the risk of an authentication request and react appropriately. Microsoft recommends the Zero Trust model is implemented over time and we can use Azure AD conditional access policies to maintain control in a mobile & cloud first world. Conditional access policies can be used to make a real-time decision on whether an authentication request is successful based on numerous factors such as:

- **Device** - is the device known/trusted/Domain joined?
- **IP** - is the authentication request coming from a known corporate IP address? Or from a country we do not trust?
- **Application** – Is the user authorized to use this application?

We can then trigger policy such as approve, trigger MFA or block authentication based on these policies.

How do I protect against viruses and malware?

Again, Office 365 provides protection for the Optimize marked endpoints in various layers in the service itself, outlined in this document. As noted, it is vastly more efficient to provide these security elements in the service itself rather than try and do it in line with devices which may not fully understand the protocols/traffic.

For the Exchange endpoints listed above, Exchange Online Protection and Office 365 Advanced Threat Protection do an excellent job of providing security of the traffic to the service.

Can I send more than just the Optimize traffic direct?

Priority should be given to the Optimize marked endpoints as these will give maximum benefit for a low level of work. However, if you wish, the Allow marked endpoints are required for the service to work and have IPs provided for the endpoints which can be used if required.

There are also various vendors who offer cloud based proxy/security solutions called secure web gateways which provide central security, control and corporate policy application for general web browsing. These solutions can work well in a cloud first world, if highly available, performant, and provisioned close to your users by allowing secure internet access to be delivered from a cloud based location close to the user. This removes the need for a hairpin through the VPN/corporate network for general browsing traffic, whilst still allowing central security control. Even with these solutions in place however, it is still strongly recommends the Optimize marked Office 365 traffic is sent direct to the service.

Why is port 80 required? Is traffic sent in the clear?

Port 80 is only used for things like redirect to a port 443 session, no customer data is sent or is accessible over port 80. This article outlines encryption for data in transit, and at rest for Office 365 and this article outlines how we use SRTP to protect Teams media traffic.
Does this advice apply to users in China using a worldwide instance of Office 365?

No it does not. The one caveat to the above advice is users in the PRC who are connecting to a worldwide instance of Office 365. Due to the common occurrence of cross border network congestion in the region, direct internet egress performance can be variable. Most customers in the region operate using a VPN to bring the traffic into the corporate network and utilize their authorized MPLS circuit or similar to egress outside the country via an optimized path. This is outlined further in this article [https://docs.microsoft.com/en-us/office365/enterprise/office-365-networking-china](https://docs.microsoft.com/en-us/office365/enterprise/office-365-networking-china)
Quick Implementation Guide for Cisco Webex Meetings

Similarly to Office 365 and Microsoft Teams, a split tunnel is required on your VPN deployment to guarantee good audio and video performance for Cisco Webex Meetings users.

All the same recommendations outlined above for split tunnelling are still valid, including using Azure Traffic Manager to send users to the nearest gateway, etc.

Webex does not support or recommend filtering IP addresses for a particular region. Filtering by region can cause serious degradation to the in-meeting experience up to and including the inability to join meetings entirely.

Webex leverages the Akamai content delivery network (CDN). The addresses akamaicdn.webex.com and ip.webex.com serve static content and are hosted by Akamai, which has IP ranges outside of the Webex IP ranges and these are subject to change at any time.

List of IP address ranges used by Cisco Webex Meeting services

<table>
<thead>
<tr>
<th>IP Address Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>64.68.96.0/19</td>
</tr>
<tr>
<td>66.114.160.0/20</td>
</tr>
<tr>
<td>66.163.32.0/19</td>
</tr>
<tr>
<td>170.133.128.0/18</td>
</tr>
<tr>
<td>173.39.224.0/19</td>
</tr>
<tr>
<td>173.243.0.0/20</td>
</tr>
<tr>
<td>207.182.160.0/19</td>
</tr>
<tr>
<td>209.197.192.0/19</td>
</tr>
<tr>
<td>210.4.192.0/20</td>
</tr>
<tr>
<td>210.4.192.0/20</td>
</tr>
<tr>
<td>216.151.128.0/19</td>
</tr>
<tr>
<td>114.29.192.0/19</td>
</tr>
<tr>
<td>69.26.176.0/20</td>
</tr>
<tr>
<td>69.26.160.0/20</td>
</tr>
<tr>
<td>62.109.192.0/18</td>
</tr>
<tr>
<td>69.26.160.0/20</td>
</tr>
</tbody>
</table>

List of Domains used by Cisco Webex Meeting Services

- *.webex.com
- *.accompany.com
- *.quovadisglobal.com

List of Domains used by Webex Teams

This domain list should also be allowed to pass outside the split tunnel, and possibly avoid proxies to further reduce the load. Generally they provide content sharing, connectivity tests, text-to-speech APIs, and performance tracking for the Webex Teams service.
For full details about all the URLs and their function, please visit this page.
**Quick Implementation Guide for Zoom**

Similarly to Office 365, Teams, and Webex, in order to obtain the best performance with Zoom, it is necessary to exclude its endpoints from the VPN tunnel and from proxies.

**List of IP address ranges used by Zoom**

<table>
<thead>
<tr>
<th>IP address range 1</th>
<th>IP address range 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.35.0/25</td>
<td>3.21.137.128/25</td>
</tr>
<tr>
<td>3.25.41.128/25</td>
<td>3.25.42.0/25</td>
</tr>
<tr>
<td>3.80.20.128/25</td>
<td>3.101.32.128/25</td>
</tr>
<tr>
<td>3.101.52.0/25</td>
<td>3.104.34.128/25</td>
</tr>
<tr>
<td>3.120.121.0/25</td>
<td>3.127.194.128/25</td>
</tr>
<tr>
<td>3.208.72.0/25</td>
<td>3.211.241.0/25</td>
</tr>
<tr>
<td>3.235.69.0/25</td>
<td>3.235.82.0/23</td>
</tr>
<tr>
<td>3.235.71.128/25</td>
<td>3.235.72.128/25</td>
</tr>
<tr>
<td>3.235.73.0/25</td>
<td>4.34.125.128/25</td>
</tr>
<tr>
<td>4.35.64.128/25</td>
<td>8.5.128.0/23</td>
</tr>
<tr>
<td>13.52.6.128/25</td>
<td>13.52.146.0/25</td>
</tr>
<tr>
<td>13.114.106.166/32</td>
<td>18.205.93.128/25</td>
</tr>
<tr>
<td>50.239.202.0/23</td>
<td>50.239.204.0/24</td>
</tr>
<tr>
<td>52.61.100.128/25</td>
<td>52.81.151.128/25</td>
</tr>
<tr>
<td>52.197.97.21/32</td>
<td>52.202.62.192/26</td>
</tr>
<tr>
<td>52.215.168.0/25</td>
<td>64.69.74.0/24</td>
</tr>
<tr>
<td>64.125.62.0/24</td>
<td>64.211.144.0/24</td>
</tr>
<tr>
<td>65.39.152.0/24</td>
<td>69.174.57.0/24</td>
</tr>
<tr>
<td>69.174.108.0/22</td>
<td>99.79.20.0/25</td>
</tr>
<tr>
<td>103.122.166.0/23</td>
<td>109.94.160.0/22</td>
</tr>
<tr>
<td>109.244.18.0/25</td>
<td>109.244.19.0/24</td>
</tr>
<tr>
<td>115.110.154.192/26</td>
<td>115.114.56.192/26</td>
</tr>
<tr>
<td>115.114.115.0/26</td>
<td>115.114.131.0/26</td>
</tr>
<tr>
<td>120.29.148.0/24</td>
<td>160.1.56.128/25</td>
</tr>
<tr>
<td>161.199.136.0/22</td>
<td>162.12.232.0/22</td>
</tr>
</tbody>
</table>
162.255.36.0/22  165.254.88.0/23  173.231.80.0/20  192.204.12.0/22
202.177.207.128/27  202.177.213.96/27  204.80.104.0/21  204.141.28.0/22
207.226.132.0/24  209.9.211.0/24  209.9.215.0/24  210.57.55.0/24
213.19.144.0/24  213.19.153.0/24  213.244.140.0/24  221.122.88.64/27
221.122.88.128/25  221.122.89.128/25  221.123.139.192/27
IPv6:
2620:123:2000::/40

- TCP Ports: 443, 8801, 8802 - for All Zoom Clients
- UDP Ports: 3478, 3479, 8801 - 8810 - for All Zoom Clients

List of IP address ranges used by Zoom Phone
8.5.128.0/24  64.211.144.0/24  103.122.166.0/23  109.94.160.0/22
120.29.148.0/24  192.204.12.0/22  209.9.215.0/24  213.19.153.0/24
213.244.140.0/24

- TCP Ports: 5090, 5091 - for All Zoom Clients
- UDP Ports: 5090, 20000 - 64000 - for All Zoom Clients

List of Domains used by Zoom
- *.zoom.us
- *.cloudfront.net

Due to the large amount of IP ranges to be supported for Zoom, please see [this page](#) - towards the bottom it's possible to download text versions of the aforementioned lists for ease of implementation.
Train your Users

Finally, after implementing the changes outlined above, it’s time to take care of helping your users make the most of their home network equipment and connectivity.

Start by explaining to your users that there are a few things they can do to improve their remote working experience in terms of networking:

- If WiFi coverage is an issue in their house, suggest to connect directly to the router via ethernet, or deploy either a mesh wifi of new generation such as Google Nest WiFi, or at least a Powerline adapter, which usually results in better, more stable speeds and pings than a bad wifi connection.

- Ask them to check in their router whether uPnP is enabled. It’s recommended to enable uPnP as most realtime applications can take advantage of this and forward ports and protocols which make the experience better. What does this mean? A router with uPnP enabled may allow an application such as Teams or Zoom to establish a high-performing UDP media stream between the remote and the local endpoint, by using STUN/TURN technologies to connect the peers directly even when behind firewalls, whereas without it, they may be forced to fall back to TCP connectivity relayed through a cloud server, thus resulting in a poor, laggy experience.

- While not strictly network related, provide your users with good business-grade headsets, handsets, speakerphones and webcams. A good, certified device will deliver better audio and video quality and be more clearly understandable even under poorer network conditions.

- Ask your users to try and avoid scheduling meetings first thing in the morning. It’s been proven that between 9 and 10am (in Europe), most cloud collaboration services seem to suffer from the highest loads. Moving your calls to less ‘prime’ hours, such as 13, and 15-18 will result in a better, more manageable experience, with less dropouts and better quality.
How to check the connection quality

There are a few websites you can use to check how good your connectivity is:

- **Office 365 Network Connectivity performance testing**: [https://connectivity.office.com](https://connectivity.office.com)
- **General network speed**: [https://speedtest.net](https://speedtest.net)
- **General network speed**: [https://fast.com](https://fast.com)
- **For more technical users, Microsoft Network Testing Companion**: [https://www.powershellgallery.com/packages/NetworkTestingCompanion/1.5.4](https://www.powershellgallery.com/packages/NetworkTestingCompanion/1.5.4)
- **For bandwidth planning**, this tool monitors user Office 365 network traffic volumes to get a clear figure for bandwidth requirements for the wider business: [https://aka.ms/bandwidth/](https://aka.ms/bandwidth/)

Obviously, because of the nature of this type of challenge, QoS and eCDN solutions such as Kollective take a step back, as most users will connect by themselves or with just 2-3 more users in their home, hence why they weren’t mentioned. And because the users should split tunnel their way into the cloud, you shouldn’t worry about QoS on your corporate network either as that traffic won’t make it onto it in the first place.