C-TAG Guidance Document

Managed Tunnels for the Deployment of Microsoft 365

Principal Author: Mark Brett

Version 2.0 June 2020

Background

Managed tunnels [8] Advice from NCSC

There are many instances where you would need to access specific services outside of a Virtual Private Network (VPN). This can be can done using managed tunnels, which is where traffic to that particular endpoint is sent outside of the configured VPN. Sensible reasons for doing this include the reduction of the load on networks caused by video conferencing services or where the function of an application requires it to communicate directly on the network, such as Wi-Fi captive portal helpers. The use of managed tunnels is only recommended in situations where the provider (of the service that will be connected to outside the tunnel) provides the following:

1. Information demonstrating that connectivity to the service uses commensurate protection to that provided by the VPN (e.g. the use of mutual Transport Layer Security authentication)

2. Definitive statements suggesting that the services use dedicated IP endpoints so that only traffic to that specific service will pass outside of the VPN

3. A business requirement for users to access the service outside of the VPN - i.e. high bandwidth services such as those used for video conferencing.

This approach is also recommended to enable Wi-Fi captive portal helpers to function.

Prerequisites:

- The process of Split Tunnelling is not supported by Windows 10 version 10 and earlier, and there are patching requirements for Windows 10 - up to 1909, all detailed here:

  https://docs.microsoft.com/en-gb/windows/security/identity-protection/vpn/vpn-office-365-optimization#version-support

- Microsoft also published their own ‘How to quickly optimise O365 traffic for remote staff’ guide here, of which the most useful document is:

  https://techcommunity.microsoft.com/t5/office-365-blog/how-to-quickly-optimize-office-365-traffic-for-remote-staff-amp/ba-p/1214571#

  This document summarises the required IP ranges for Teams Only and for all of Office 365 so you do not have to look them up through the large Office 365 IP Ranges list.

- For Split Tunnelling to be fully effective, Proxy PAC or WPAD files should also be configured to bypass proxy for these O365 IP ranges. While Teams UDP traffic will not observe Proxy rules, some apps like Outlook do. Examples of how to configure this are in Paul Collinge's (Microsoft) blog post here in the comments (03-12-2020 02:30 PM):

  https://techcommunity.microsoft.com/t5/office-365-blog/how-to-quickly-optimize-office-365-traffic-for-remote-staff-amp/ba-p/1214571#

- Authentication must also be considered for effectiveness. In an ADFS or Hybrid Azure AD environment, authentication may reasonably be expected to still go via the AOVPN tunnel, which reduces complexity but means while traffic optimisation is achieved, full resilience in the event of loss of AOVPN is not. In a pure Azure AD environment, authentication may be direct to the Tenant, in which case both traffic optimisation and full independence of the AOVPN service is achieved, but administrators must ensure that external authentication to the Tenant is configured e.g. using Conditional Access and/or Multi-Factor authentication.

- As discussed in the above article, when Windows Firewall have been configured to control outgoing traffic from the workstation, then they too should be allowed to the subnets and TCP AND UDP ports.

Advice and Guidance

As per the disclaimer below, we have provided signposting to trusted advice from third parties, including the National Cyber Security Centre (the UK's National Technical Authority for Cyber Security and Information Assurance). All the sources are referenced below, and it is suggested the reader download those documents and understand them thoroughly or engage a third-party solutions architect to do so. Data Privacy requirements must always be considered and the organisation's Senior Information Risk Officer (SIRO) must sign off on any residual business risks.

All solutions must also consider P3T (Personnel, Physical, Procedural and Technical) risks.

When implementing a VPN split tunnelling solution for MS365, access will also require staff training, guidance and procedures on how to use correctly, supported by a policy (for example, one will only access the corporate MS365 via an authorised device i.e. using the corporate VPN etc). This will mean you need to ensure corporate policies are updated accordingly such as the following:

- Acceptable Usage Policy
- End User Device Policy
- Home Working Policy
- Email and Internet Access Policies

The solution will need a Data Protection Impact Assessment (DPIA), as Personally Identifiable Information (PII) is transmitted and received over the link. This may mean the Corporate Risk Register needs to be updated and an Information Risk Assessment is recommended.

Microsoft and others have provided detailed guidance and the recommended approach is to have an Information Governance Framework in place; you should start with the NCSC Cloud Security Principles. This gives an overarching framework that covers the technical requirements for a good cloud services provider. Microsoft have published a Cloud Principles assertion document [3], that details how MS365 meets the NCSC Cloud Principles [1]. The second Microsoft document provides detailed guidance on how to implement the cloud Principles [4], and provides a policy framework checklist.

Identified Technical Issues/Deficiencies/Observations to Consider

This document may be used by organisations of different sizes and structures so generic guidance will always need reading in context. The following should be considered:

- A technical issue has been identified with this configuration, the Edge browser now fails to connect to O365 and Azure services when directly routed, however Chrome continues to work. Investigations thus far have pointed to an IPv6 issue or an authentication issue, this issue is not yet resolved. Source: Norfolk CC

- Traversing home consumer infrastructure introduces the potential for traffic to be intercepted and manipulated by malicious intermediaries. Source: Hull CC

- The guidance does not address the issue where Microsoft also recommends bypassing all security infrastructure within a corporate LAN - i.e. inside a local network that has nothing to remote sites.

- The material does not consider the issue of O365 context, where differing products and configuration provide differing levels of protection against malicious code. Source: Hull CC

- Split tunnelling removes several layers of anti-malware security that are normal for every other web site. Source: Hull CC

- Insecure O365 packages/configuration increases the risk that malicious content may directly attack an endpoint within prior inspection by corporate network defences. Source: Hull CC

- The guidance does not consider the client context, where the walled garden model exists in order to offset deficiencies in the security of certain mobile platforms. Source: Hull CC

- It is likely that this case will create a precedent that will lead to exemption for other bandwidth-heavy web sites including but not limited to: Webex, Zoom, Brightcove, YouTube, etc. Source: Hull CC

- Expansion of split tunnels will result in a corresponding increase in risk exposure. Source: Hull CC

- Both documents cite supporting material with an undue emphasis on Microsoft guidance, and fail to include highly respected and authoritative independent security sources. Source: Hull CC

- The increased risk exposure caused by split tunnelling should at a minimum lead to implantation of heightened security posture on remaining system components as mitigation. Source: Hull CC

VPN Tunnelling Specifics

Explainer video [6]

The specific MS365 VPN Tunnelling Guidance explains the way the technology works and the steps needed to implement it securely.

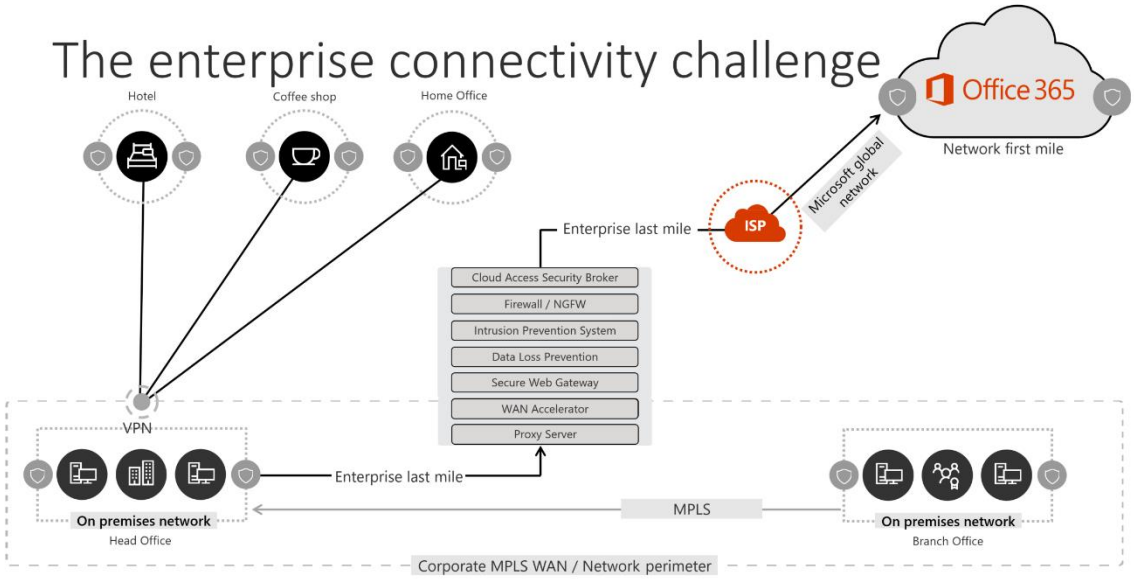

Figure 1: A VPN split tunnel solution with defined Office 365 exceptions sent directly to the service. All other traffic traverses the VPN tunnel regardless of destination.
Source: https://docs.microsoft.com/en-us/office365/enterprise/office-365-vpn-implement-split-tunnel

The recommended solution specifically targets Office 365 service endpoints categorised as **Optimize** in the topic Office 365 URLs and IP address ranges. Traffic to these endpoints is highly sensitive to latency and bandwidth throttling and enabling it to bypass the VPN tunnel can dramatically improve the end user experience as well as reduce the corporate network load. Office 365 connections that do not constitute the majority of bandwidth or user experience footprint can continue to be routed through the VPN tunnel along with the rest of the Internet-bound traffic. For more information, see the VPN split tunnel strategy.

- Preserves the security posture of customer VPN implementations by not changing how other connections are routed, including traffic to the Internet.
  The recommended configuration follows the **least privilege** principle for VPN traffic exceptions and allows customers to implement split tunnel VPN without exposing users or infrastructure to additional security risks. Network traffic routed directly to Office 365 endpoints is encrypted, validated for integrity by Office client application stacks, and scoped to IP addresses dedicated to Office 365 services which are hardened at both the application and network level. For more information, see alternative ways for security professionals and IT to achieve modern security controls in today's unique remote work scenarios (Microsoft Security Team blog).

- Is natively supported by most enterprise VPN platforms. Microsoft continues to collaborate with industry partners producing commercial VPN solutions to help partners develop targeted guidance and configuration templates for their solutions in alignment with the above recommendations. For more information, see HOW TO guides for common VPN platforms.

For full implementation guidance, see:
Implementing VPN split tunnelling for Office 365.

Source: https://docs.microsoft.com/en-us/office365/enterprise/office-365-vpn-split-tunnel

Disclaimer:

This document was produced by bringing together guidance from trusted government agencies, providers and third parties. The information contained in it is accurate and technically correct at the point of publication. Any application of the guidance is solely the discretion of the reader. The authors are not responsible for any consequences of applying the guidance.

Glossary:

DPIA	Data Protection Impact Assessment
MS365	Microsoft 365, the new name for Office 365
O365	Office 365 Microsoft Office, the cloud-based productivity suite, now called MS365
PII	Personally Identifiable Information under the Data Protection Act
Tunnelling	VPN Tunnelling
VPN	Virtual Private Network turns part of an unsecure connection into a secure point-to-point connection.

Related Microsoft guidance:

Implementing VPN split tunnelling for Office 365
Office 365 performance optimization for China users
Alternative ways for security professionals and IT to achieve modern security controls in today's unique remote work scenarios (Microsoft Security Team blog)
Enhancing VPN performance at Microsoft: using Windows 10 VPN profiles
Running on VPN: How Microsoft is keeping its remote workforce connected
Office 365 Network Connectivity Principles
Assessing Office 365 network connectivity
Microsoft 365 connectivity test

References:

[1] https://www.ncsc.gov.uk/collection/cloud-security/implementing-the-cloud-security-principles
[2] https://news.microsoft.com/en-gb/2019/01/07/government-backs-office-365-cloud-move-after-microsoft-guidance/
[3] https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE2MCCr
[4] https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE2MHP5
[5] https://docs.microsoft.com/en-us/office365/enterprise/office-365-vpn-split-tunnel
[6] https://youtu.be/Z68w2uOUoAE
[7] https://www.ncsc.gov.uk/blog-post/introducing-new-guidance-virtual-private-networks-vpns
[8] https://www.ncsc.gov.uk/collection/mobile-device-guidance/virtual-private-networks

NB: All links correct as of June 2020.