Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Using Virtual Private Networks

JUNE 2020

Introduction

Virtual Private Network (VPN) connections can be an effective means of providing remote access to a network; however, VPN connections can be abused by an adversary to gain access to a network without relying on malware and covert communication channels.

This document identifies security controls that should be considered when implementing VPN connections. This document does not discuss the different technologies involved in establishing VPN connections, the protocols and algorithms used to secure VPN connections, or how to establish VPN connections.

For the purpose of this document, the term 'site-to-site VPN' is used to refer to a connection between two networks, either via dedicated communications links or over the internet, while the term 'remote access VPN' is used to refer to users connecting to a network from an offsite location over the internet.

User accounts

User accounts for VPN connections should be separate from standard user accounts. This will limit the activities that can be performed by an adversary should a VPN user account be compromised.

Further, the permissions applied to VPN user accounts should be restricted to each user's required level of access. This will minimise the severity of a successful compromise. VPN user accounts with minimum permissions, that can only perform basic operations on a network, will also impede the ability of an adversary to gain a foothold on a network.

Finally, access to applications, servers and shared resources on a network should only be granted where necessary for users to perform their duties. For example, if a user only needs access to email services, they should be denied access to file servers.

Multi-factor authentication

Adversaries frequently attempt to steal credentials to compromise a network. These credentials allow them to easily propagate on a network and conduct malicious activities without installing additional exploits, thereby reducing the likelihood of detection. Adversaries also frequently attempt to steal credentials for VPN connections as this can further mask their activities.

Multi-factor authentication should be used for VPN connections. When multi-factor authentication has been implemented correctly, it is more difficult for an adversary to successfully exploit a network, as several authentication factors for accounts need to be compromised to gain access.

Device authentication

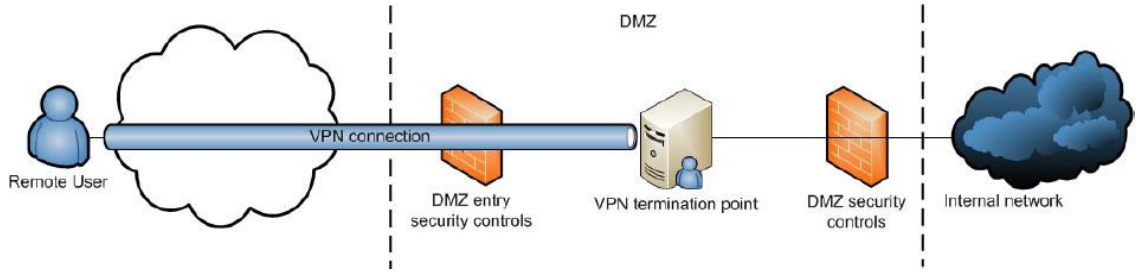
Device authentication ensures that a device establishing a VPN connection is approved for such purposes. Device authentication is applicable to both site-to-site VPNs and remote access VPNs, and typically takes the form of a certificate issued to a device. The device, and by extension the device certificate, may or may not be tied to a specific user.

If a VPN endpoint receives a connection request, it should authenticate the device in addition to the user. The VPN connection should be terminated if either device or user authentication fails. A connection attempt from an unauthenticated device should be considered suspicious and logged for further investigation.

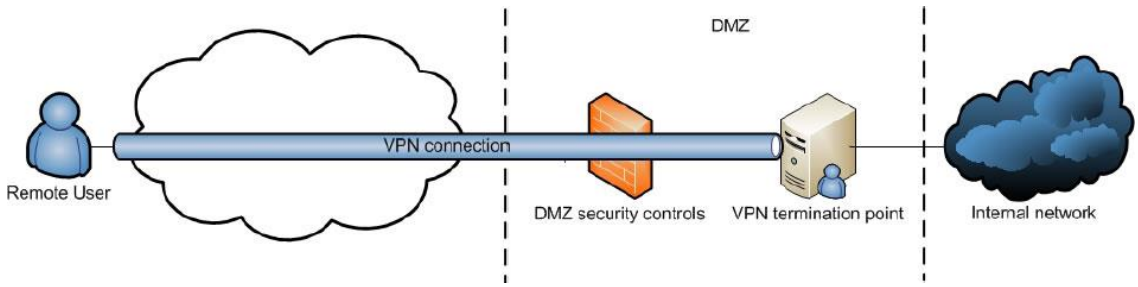
VPN termination points

Devices used for VPN connections have the same potential for compromise as corporate workstations. If a device using a VPN connection is compromised there is the security risk it could be used to compromise connected networks. Because of this, all VPN traffic should be treated as untrusted and potentially malicious, and subjected to the same scrutiny as any external communications. To this end, VPN termination points should be within a DMZ to allow for the proper inspection and auditing of unencrypted VPN traffic prior to entering and leaving a network.

The following diagram shows a simplified example of a proper VPN connection termination within a DMZ.



The following diagram shows a simplified example of an improper VPN connection termination within a DMZ.



Split tunnelling

Devices accessing a network via a VPN connection should disable split tunnelling. Split tunnelling allows a device to be simultaneously connected to an organisation's network and directly to the internet. Organisations should ensure that web browsing from a device connected to a VPN connection is conducted through their internet gateway rather than via a direct connection to the internet. If a device used for VPN connections has already been compromised, split tunnelling could allow an adversary to interact with the organisation's network in real time making it easier for an adversary to achieve their goals.

Controlling connection sources

If a site-to-site VPN implementation supports the control of connection sources, a list of approved MAC or IP addresses should be implemented to only allow VPN connections from approved sources. This will prevent unauthorised connection attempts even when legitimate credentials have been provided.

If a site-to-site VPN implementation does not support the control of connection sources, VPN connection log entries should be monitored for anomalies. If a non-approved source appears in the VPN connection logs, it should be treated as suspicious and logged for further investigation.

Effective logging and log analysis

Effective logging and log analysis of VPN connections is vital to accounting for activities performed on a network. Effective logging also provides a central repository of information in the event of an attempted or successful compromise. Effective log analysis further aids in finding malicious and other unauthorised activities in a timely manner.

VPN connection information which should be logged, where available, includes:

- Authentication information – Any certificate information provided when a VPN connection is made using a certificate, VPN user account credentials, and any information about the remote host and time of any failed authentication attempts.
- Session information – The establishment time of a VPN connection, the duration of the connection and the amount of data transferred.
- Activities performed – The activities performed by the VPN users, especially those relating to sensitive resources.
- Remote host information – Any identifying information about the remote host such as the operating system, IP address, MAC address and the hostname.

Further information

The ***Australian Government Information Security Manual*** (ISM) assists in the protection of information that is processed, stored or communicated by organisations' systems. It can be found at https://www.cyber.gov.au/acsc/view-all-content/ism.

The ***Strategies to Mitigate Cyber Security Incidents*** complements the advice in the ISM. The complete list of strategies can be found at https://www.cyber.gov.au/acsc/view-all-content/publications/strategies-mitigate-cyber-security-incidents.

Additional information regarding multi-factor authentication can be found in the ***Implementing Multi-Factor Authentication*** publication at https://www.cyber.gov.au/acsc/view-all-content/publications/implementing-multi-factor-authentication.

Addition information regarding remote access clients can be found in the ***Using Remote Desktop Clients*** publication at https://www.cyber.gov.au/acsc/view-all-content/publications/using-remote-desktop-clients.

Contact details

If you have any questions regarding this guidance you can contact us via 1300 CYBER1 (1300 292 371) or https://www.cyber.gov.au/acsc/contact.