

APRIL 2013



# Additional Security Considerations and Controls for Virtual Private Networks

## Introduction

1. A Virtual Private Network (VPN) can be an effective means of providing remote access to a corporate network or resources; however, VPN connections can be abused by an adversary to gain access to a corporate network without relying on malware and covert communication channels. To reduce this security risk, it is important to implement appropriate security controls on VPN connections and end points to prevent and detect malicious activities.

2. This document identifies security controls that should be considered when implementing a VPN to prevent or detect malicious activity. This document will not discuss the different technologies involved in establishing a VPN connection, the algorithms and ciphers used to secure a VPN connection, or how to establish a VPN connection.

3. For the purpose of this document, the term 'site-to-site VPN' will be used to refer to a VPN which is used to establish a connection between two corporate networks, either via dedicated communications links or over the Internet. The term 'remote access VPN' will be used to refer to a VPN which allows users to connect into a corporate network, most commonly from an offsite location over the Internet.

## Multi-factor User Authentication

4. Cyber adversaries frequently attempt to steal legitimate user or administrative credentials when they 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 and making it easier for less sophisticated adversaries. Cyber adversaries will also try to gain credentials for remote network access solutions, including VPNs, as these accesses can mask their activities and reduce the likelihood of being detected.

5. Multi-factor user authentication should be enabled on remote access VPN solutions. When multi-factor user authentication has been implemented correctly on a network, it is more difficult for a cyber adversary to successfully exploit the network, as both authentication factors for an account need to be

compromised to gain access. Additional information regarding multi-factor authentication can be found in ASD's *Multi-factor Authentication*[1] publication.

## Device Authentication

6. Device authentication ensures that a device connecting to a VPN is legitimate and approved for use on the network. Device authentication is applicable to both remote and site-to-site VPN solutions, and should be implemented in addition to multi-factor user authentication where possible.

7. Device authentication typically takes the form of a certificate issued to the device. The device, and by extension the device certificate, may or may not be tied to a specific user.

8. If the VPN endpoint receives a VPN 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 User Account Permissions

9. The permissions applied to VPN user accounts need to be strictly locked down and limited to only allow the required level of access in order to minimise the severity of a successful compromise. VPN user accounts with only minimum permissions, and which can only perform basic operations on the network, will impede the ability of an adversary to gain a foothold on the corporate network.

10. The following restrictions of permissions should be considered:

    a. **Programs and commands –** Access to programs and commands on the network should only be given where necessary. For example, if a user has no need to use a remote desktop through the VPN connection, then all access to remote desktop programs should be removed for those accounts.

    b. **Folder and server access –** Access to servers on the network and shared resources should only be allowed when it is necessary and needed. For example, a VPN user who only needs access to email should be denied access to the file server.

    c. **Admin login –** ASD's ISM advises that privileged accounts:

        i. Should not be allowed to remotely access organisational systems containing UNCLASSIFIED or PROTECTED government data.
        ii. Must not be allowed to remotely access organisational systems containing data classified higher than PROTECTED.

[1] http://www.dsd.gov.au/publications/csocprotect/multi_factor_authentication.htm

## VPN Termination Points

11. It is likely that a device used for VPN remote access would have at least the same potential for compromise as a corporate desktop, most likely higher due to the potential difficulties associated with patching and other device administration constraints.

12. If a machine is compromised there is the security risk that the machine could be used to directly compromise the corporate network. 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 the corporate network.

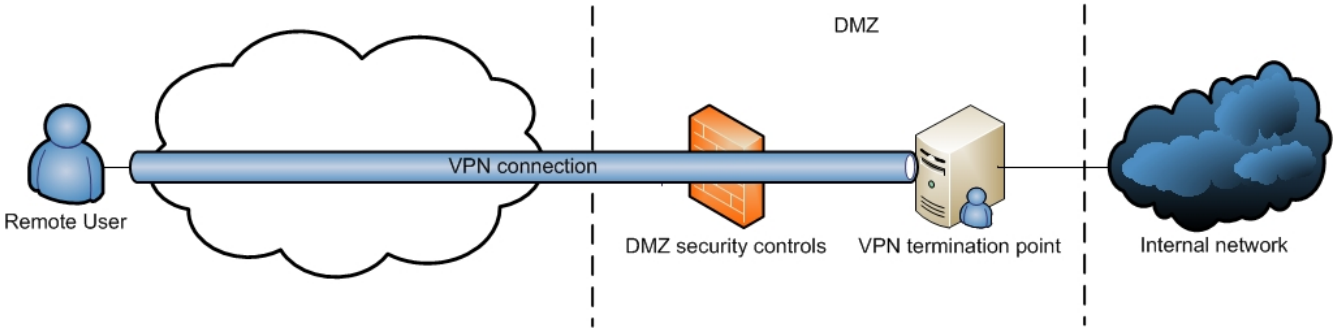


**Figure 1 Simplified example of an improper VPN connection termination end point within the DMZ**

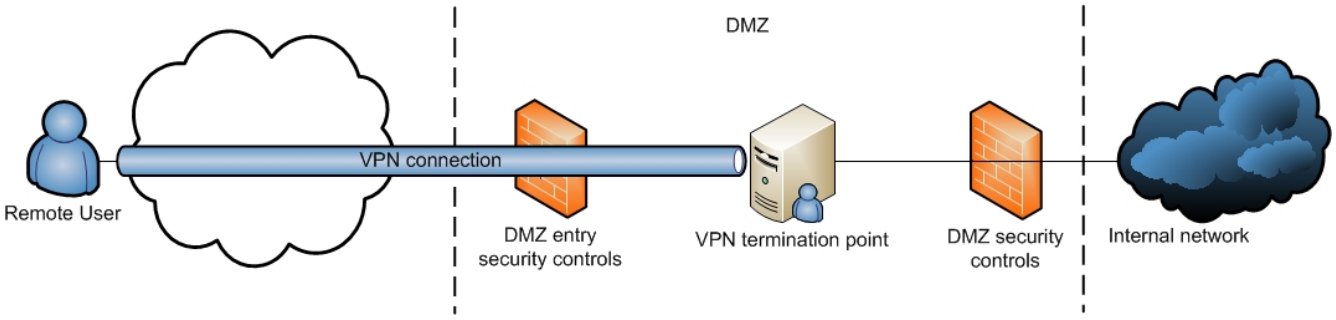


**Figure 2 Simplified example of a proper VPN connection termination end point within the DMZ**

## Split Tunnelling

13. ASD's ISM advises that a device accessing an organisational system via a VPN must disable split tunnelling. Split tunnelling allows a machine to be simultaneously connected to both a corporate network via a VPN connection and to another network, such as the Internet. Organisations should ensure that web browsing from a device connected to the VPN is through their internet gateway rather than via a direct connection to the Internet. If a remote access VPN machine has already been compromised, split tunnelling, particularly if simultaneously connected to the Internet, could allow an

adversary to interact with the corporate network in real time making it easier for an adversary to achieve their goals.

## Time Based Logins

14. Access should only be allowed during certain times, depending on business requirements, for remote access VPNs. This security control should be enforced such that a VPN user account can only connect within the allowed connection window with all unsuccessful attempts logged.

15. By only allowing access to the VPN during specified time blocks, suspicious access attempts or logons can be identified. This also creates an access baseline for security auditing the connections of a particular user or account type.

## Connection Location Limitation

16. If a site-to-site VPN implementation supports it, a whitelist 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.

17. If the VPN implementation does not support source MAC or IP address whitelisting, monitoring of VPN connection log entries can be conducted. If a non-approved source appears in the VPN connection logs, it should be treated as suspicious and logged for further investigation.

18. For example, a site-to-site VPN connection is established between two corporate sites. The IP addresses of the endpoints are both known and static. As such, if an endpoint sees a connection request which does not match the defined IP of the other endpoint, this request should be dropped even if the supplied credentials are correct.

## Extensive Logging and Log Analysis

19. Logging and log analysis of VPN connection information is vital to be able to account for actions performed on a network and any networks connected to it via a VPN. Effective logging also provides a central repository of information in the event of an attempted or successful compromise. Effective log analysis will aid in finding malicious and other unauthorised access and activities in a timely manner. The VPN connection information which ASD considers helpful and recommends should be logged, where available, includes:

a. **Authentication information –** All relevant information regarding authentication should be logged including:

   i. **Certificate information –** Any identifying information provided when a VPN connection is made using a certificate e.g. usernames.
   ii. **Time of login –** The time of establishing a VPN connection and the duration of the connection along with the amount of data that was transferred in that time frame and the account credentials used to establish the connection.

iii. **Failed connection attempts –** When an unsuccessful connection occurs, any information about the remote host and the time of the failed connection attempt.

b. **Actions performed –** The actions performed by the connected VPN users on sensitive resources. This will provide an audit trail of the VPN users actions on the network.

c. **Remote host information –** Any identifying information about the remote host such as the operating system, IP address, the MAC address, and the hostname.

## VPN User Account Separation and Credential Management

20. VPN user accounts should be separated from corporate network user accounts. As such, corporate network user accounts will not be able to be used to connect to remote access VPNs. Separation of corporate network user accounts from those used for VPN access will limit the access and activities that can be performed by an adversary should an account become compromised.

21. Just like local and domain user credentials, remote VPN user credentials should be renewed and changed on a regular basis. This will restrict the continual reuse of compromised VPN user account credentials as it will require the VPN user account to be compromised repeatedly. For example, if an adversary does compromise a VPN user's credentials, forcing the user to regularly change their VPN credentials means that these credentials will no longer work and the adversary will lose access to the VPN.

## Further Information

22. Further information on approved encryption ciphers and algorithms, split tunnelling and user account security can be found in the *Australian Government Information Security Manual* (ISM)[2].

23. Additional information on log analysis can be found in *Strategies to Mitigate Targeted Cyber Intrusions – Mitigation Details* [3].

24. An example case study of why log analysis is essential can be found on the Verizon security blog[4].

## Contact Details

Australian government customers with questions regarding this advice should contact ASD Advice and Assistance at asd.assist@defence.gov.au or by calling 1300 CYBER1 (1300 292 371).

Australian businesses or other private sector organisations seeking further information should contact CERT Australia at info@cert.gov.au or by calling 1300 172 499.

[2] http://www.dsd.gov.au/infosec/ism
[3] http://www.dsd.gov.au/infosec/top-mitigations/top35mitigation-details.htm
[4] http://verizonenterprise.com/security/blog/index.xml?postid=1626