



Virtual Private Network (VPN)

Introduction

The COTS Security Guidance Virtual Private Network (VPN) describes the usage and the Security issues in using a VPN connection.

Overview

A VPN connection is a tool that extends a network through an independent Internet connection.

A VPN connection gives the opportunity to an employee to access folders, files and emails. With security and encryption tools, a VPN connection allows the employee to work safely from an offsite location such as home (telework), hotels or other department sites.

Technology

A VPN provides the ability to work remotely as if the employee was sitting at their office desk. The secure channel created by the VPN is encrypted and protects the confidentiality and integrity of the network.

Security and Risks

The VPN must be secured and monitored to prevent cyber attacks. Also, the employee using a VPN must be made aware of the risks and understand the potential threats.

Features

Confidentiality Transmitted data should always be encrypted.

Integrity The VPN should be able to verify that the transmitted data has not been altered.

Secure Authentication Is required for remote access to the VPN.

Host Security A compromised remote client may be used for unauthorized access to the VPN network.

