Communications Security Establishment
Centre de la sécurité des télécommunications

UNCLASSIFIED

CANADIAN CENTRE FOR CYBER SECURITY

Virtual private networks

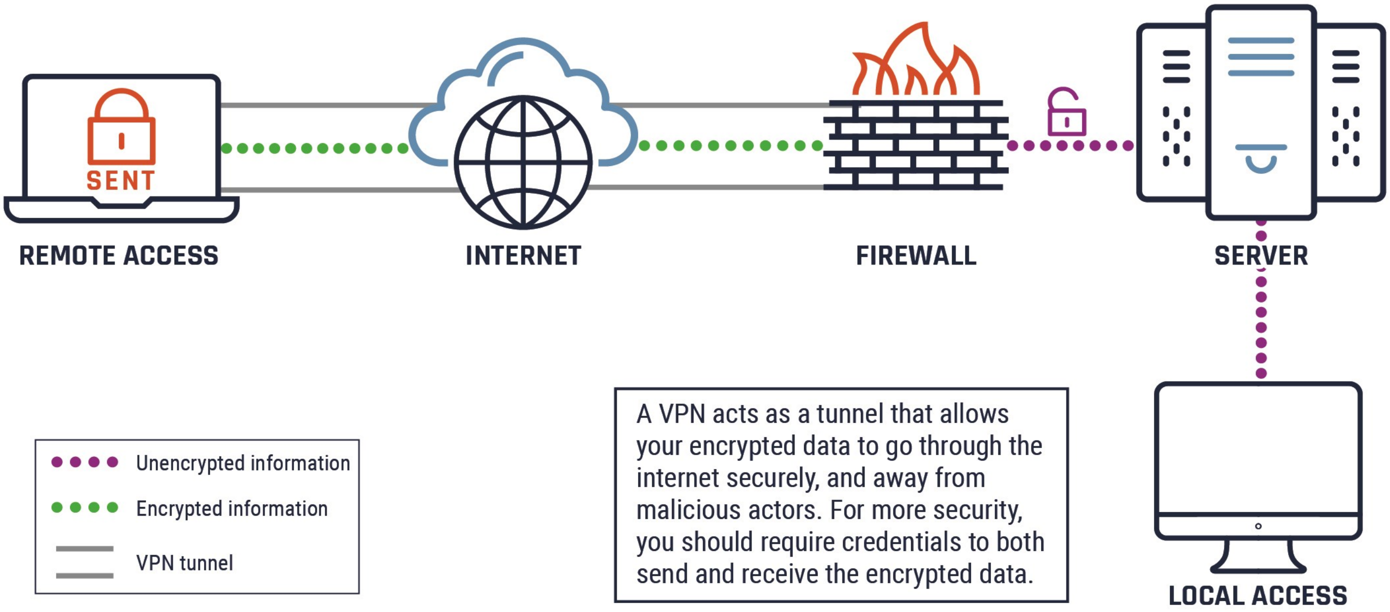
OCTOBER 2019

ITSAP.80.101

A virtual private network (VPN) is a secure connection between two points, such as your laptop and your organization's network. A VPN acts as a tunnel that you can use to send and receive secure data on an existing physical network. For example, a telework employee can use a VPN to send data that is encrypted until it reaches its destination (e.g. work server, teleworker). In this document, we introduce some of the risks and considerations your organization should understand before using VPN services.

How do VPNs work?

The figure below shows how a remote user sends encrypted data to their organization's server using a VPN. The encrypted data is sent through a "tunnel" that protects it from threat actors. In this figure, we assume that the VPN tunnel ends once the data arrives at the organization's firewall or VPN gateway. Most VPN gateways are built into the firewall. In this figure, the end point of the data transfer is a specific server, which is accessed by a user. This user should be required to enter credentials to access the encrypted data on the organization's network.



A VPN acts as a tunnel that allows your encrypted data to go through the internet securely, and away from malicious actors. For more security, you should require credentials to both send and receive the encrypted data.

AWARENESS SERIES

© Government of Canada
This document is the property of the Government of Canada. It shall not be altered, distributed beyond its intended audience, produced, reproduced or published, in whole or in any substantial part thereof, without the express permission of CSE

What types of VPNs exist?

Gateway-to-gateway: Used to connect two networks by creating a VPN over a public network, and securing all of the traffic between them. Typically used to connect remote office sites.

Host-to-gateway (remote-access): Used to provide remote access (such as a remote worker's laptop or mobile device) to an enterprise network.

Host-to-host: Similar to remote-access VPN, but connecting a host to a specific resource on an enterprise network or another specific host.

Third-party privacy: Used to secure a connection from a public access point (such as an airport or hotel Wi-Fi hotspot) to a third party VPN provider. The provider then redirects the user's traffic to make it appear to originate from the third-party's network.

How can I protect the data being sent or accessed through a VPN?

Your organization should assess what data is sent and accessed through a VPN and the value of this data to understand the risks associated with using a VPN. Your organization should have clear policies for employees who use a VPN to remotely access a work server.

If possible, the configuration settings should require individuals receiving the encrypted data to enter authentication credentials in order to access the information. Having two separate keys or credentials for encryption and decryption is called asymmetric cryptography.

What are the risks?

VPNs can introduce security risks to your organization. Your organization should research a VPN service before purchasing it to ensure it is inline with their policies. Your organization may have increased levels of risks due to the following examples:

- If you choose to use an untrusted network (e.g. free Wi-Fi) or if there is malicious software on the organization's network, a VPN may not be able to provide the level of security you are hoping for
- If you disclose your encryption key or it is stolen, the security of your information will be jeopardized
- It is important to note that some VPN services are focused on masking your identity online, rather than protecting your data

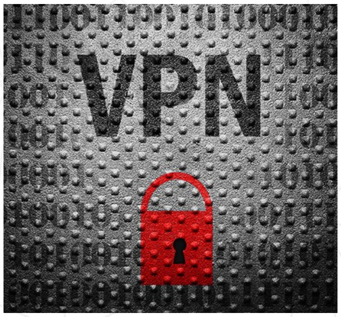
What factors need to be considered when using a VPN?

When using a VPN service in your organization, you should consider the following recommendations:

- Use a hardware token that can't be copied (e.g. RSA token) as an added layer of security
- Use multi-factor authentication to add another layer of security
- Avoid logging into sensitive accounts unless you are using a VPN
- Ensure employees use secure Wi-Fi (and avoid free Wi-Fi) when using a VPN
- Many free and paid VPN services exist. Choose one that is best suited for your organization's needs (e.g. size, cost)

Learn more

- Selecting and Hardening Remote Access VPN Solutions (PDF)
- Device Security Guidance - Virtual Private Networks (VPNs)



Need help or have questions? Want to stay up to date and find out more on all things cyber security?
Come visit us at Canadian Centre for Cyber Security (CCCS) at **cyber.gc.ca**