# Virtual private networks

CANADIAN CENTRE FOR CYBER SECURITY
June 2024 | ITSAP.80.101

A virtual private network (VPN) is a secure connection between 2 points, such as your laptop and your organization's network. A VPN acts as a tunnel to send and receive secure data on an existing physical network. For example, a remote employee can use a VPN to encrypt data as it travels through the network to its destination. That destination can be another remote worker, a corporate office or other work servers. This publication introduces some of the risks and considerations when using a VPN.

## How virtual private networks work

A VPN conceals incoming and outgoing data through a secure tunnel. This data can be decrypted once it reaches its intended destination. VPN tunnels mask your data and IP address and other personal information while you are accessing the Internet.

A VPN can encrypt the data at both endpoints. Some VPNs can also encrypt the data while it is in transit. This allows traffic to be secure as it passes between gateways through the tunnel. For a higher level of security, your organization should consider using a VPN that encrypts data while in transit.

Most VPN gateways are built into a firewall. In many cases, the endpoint of the data transfer is a specific server, which is accessed by a user. Your organization should require users to enter their credentials to access the encrypted data on your network. For a higher level of security, your organization can require users to enter credentials to both send and receive encrypted data.

## Types of virtual private networks

There are various types of VPN your organization can consider.

**Gateway-to-gateway:** Used to connect 2 networks by creating a VPN over a public network and securing traffic between them. This type of VPN is typically used to connect remote office sites.

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

**Host-to-host:** Used to connect 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.

## Risks of using a virtual private network

VPNs can introduce security risks to your organization. Before purchasing a VPN service, your organization should do research and ensure the VPN service aligns with its policies. Your organization may have increased levels of risk due to the following circumstances:

- A VPN may not be able to provide the desired level of security if you choose to use an untrusted network, such as free Wi-Fi or if there is malicious software on the organization's network
- The security of your information will be jeopardized if your encryption key is compromised
- Some VPN services are focused on masking your identity online rather than protecting your data

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada



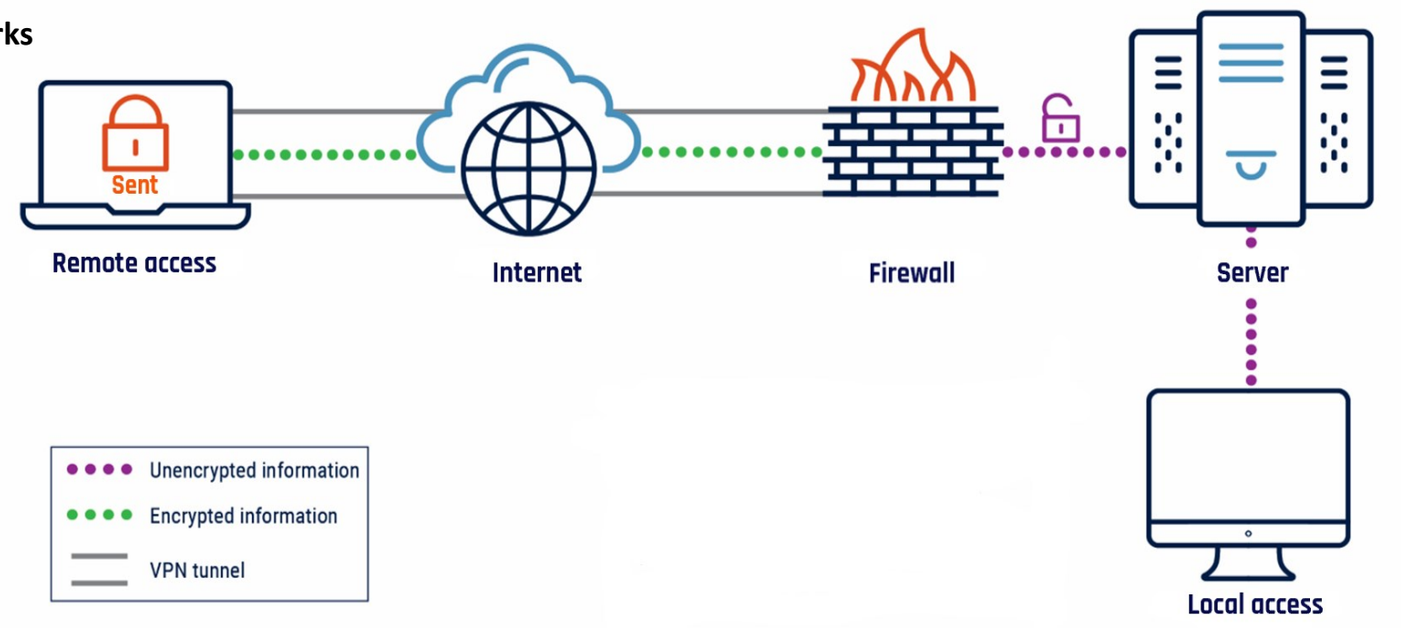
Canada

## Choosing a virtual private network

Before choosing a VPN, your organization should assess its business needs and capabilities and weigh the risks. You must also consider 2 categories of VPN security protocols: Internet Protocol Security (IPsec) and Transport Layer Security (TLS). Protocols determine how data is sent, received and secured. For example:

- With **IPsec**, your data and the tunnel it travels through are encrypted. This makes it harder for threat actors to get your data. It requires authentication at both ends to send and receive data over this VPN.
- With **TLS**, only the tunnel through which the data travels is encrypted. If a threat actor is able to break the encryption of the tunnel, your data is no longer protected.

**Figure 1: How an IPsec VPN works**




While both categories of protocols offer confidentiality, integrity and authenticity, they do so in different ways and to different degrees. One of the key differences between IPsec and TLS is where they operate within the Open System Interconnection (OSI) model. There are 7 layers to OSI, with each performing a different function. The lower the OSI layer number in which the VPN operates, the more secure and further it will be from threat actor reach. TLS operates in layers 4 through 7 (transport layer) and IPsec operates in layer 3 (network layer). Your IT department should assess the specific security needs of your organization before choosing a VPN protocol framework. IPsec is recommended for site-to-site access. It can take more effort to set up but offers enhanced cyber security. TLS is better for easy remote access with low set up requirements. Consult the comparative lists below to learn more about each VPN protocol.

## Internet Protocol Security

- Supports gateway-to-gateway and host-to-gateway connection
- Operates at OSI layer 3 and above and uses authentication protocols that require a pre-shared key from the client and server
- Encrypts your data at start and end points as well as in transit, offering full end-to-end encryption
- Is typically used only on corporate-issued devices due to security requirements
- Requires installation of a client application on users' end device
- Offers a high level of security as it has a smaller attack surface
- Runs tasks within the operating system Kernal
- Inhibits adversary-in-the-middle attacks by using shared secret authentication
- Allows you to check the packet for malware before opening at the receiving end
- Allows you to access your organization's network resources, such as applications, portals and internal servers, as if you were onsite
- Provides computer-to-computer communications while encrypting entire network packets

## Transport Layer Security

- Supports host-to-gateway connection
- Operates on layers 4 through 7 of the OSI model
- Provides encryption from the sender to a specified target, but does not provide full end-to-end encryption
- Can be used on any end device, such as a personal laptop, on any operating system and in any location
- Does not require application download as most browsers are already set up to support TLS
- Has less robust security compared to IPsec as its tasks are run from the user space in the transport and application layers
- Performs tasks at a more exposed layer which is easier to hack
- Offers limited productivity as you are only connected to your organization through a browser
- Offers customized access controls per user

## Protecting your data when using a virtual private network

Your organization should assess the type and value of data being sent and accessed through a VPN to understand the associated risks. You should implement clear policies for employees using a VPN to remotely access corporate servers.
Having 2 separate keys or credentials for encryption and decryption is called asymmetric cryptography. If possible, you should configure your VPN to use asymmetric cryptography. This requires users receiving encrypted data to enter authentication credentials to access the information.

When using a VPN service, your organization should consider:

- using a hardware token that can't be copied, such as an RSA SecurID token, for an added layer of security
- activating multi-factor authentication
- asking employees to only access sensitive accounts if using a VPN
- ensuring employees use secure Wi-Fi and avoid public Wi-Fi when using a VPN

### Learn more

- Using encryption to keep your sensitive data secure (ITSAP.40.016)
- Steps for effectively deploying multi-factor authentication (MFA) (ITSAP.00.105)
- Wi-Fi security (ITSP.80.002)
- Guidance on securely configuring network protocols (ITSP.40.062)
- Guidance on using tokenization for cloud-based services (ITSP.50.108)

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada



Canada