Université Batna 2

Virtual Private Networks (VPN)
Réseaux privés virtuels

Chapter 7

Préambule

Une vingtaine d'années auparavant, les systèmes d'information d'entreprises étaient plutôt

- **centralisés**,
- **basés sur des échanges de papiers**,
- **sans accès distants**.

Aujourd'hui, les SI d'entreprises sont plutôt **distribués sur plusieurs sites**:
on retrouve notamment **un siège principale** et

- des **filiales**,
- des **télé-travailleurs**,
- des **commerciaux**,
- etc.

Préambule

L'accès distant devient alors indispensable pour supporter cette décentralisation et la mondialisation des échanges.

Ceci devient plus important avec les **nouvelles technologies sans fils** et la **forte intrusion d'Internet** dans notre société.

Préambule

Après avoir vu comment protéger votre réseau à l'aide de

- **FW (stateless, statefull, proxy, reverse proxy/WAF, NGFW)**
- **IDS/IPS (HIDS/HIPS, NIDS/NIPS)** et
- **PKI:** comment s'assurer que votre identité ou l'identité des autres entités avec lesquelles vous communiquez est authentique de façon électronique.

Dans ce chapitre, nous allons voir comment sécuriser une connexion entre deux LAN distants.

Ceci est permis à l'aide de l'utilisation de **VPN**.

Préambule

Exemple

Une entreprise centrée à Alger ou Batna possède plusieurs filiales dans le monde ou dans plusieurs villes Algériennes.

Afin que tous les utilisateurs de toutes les filiales puissent accéder au réseau local de l'entreprise de façon sécurisée, l'utilisation d'un r**éseau privé virtuel** est une nécessité.

En résume, **c'est un besoin des entreprises de relier ses différents sites**, d'où le besoin de **créer des VPN**.

Réseaux privés virtuels

Définition

Qu’est-ce qu’un VPN?

Réseaux privés virtuels

Définition

Qu’est-ce qu’un VPN?

Un **réseau privé virtuel** (VPN) en anglais **Virtual Private Network**

- Un système permettant de
  - faire **communiquer** ensemble **les postes des différents sites** d'une société
  - tout **en assurant un moyen sécurisé d'acheminement** des données échangées **empruntant les réseaux de télécommunication publics**.

Réseaux privés virtuels

Définition

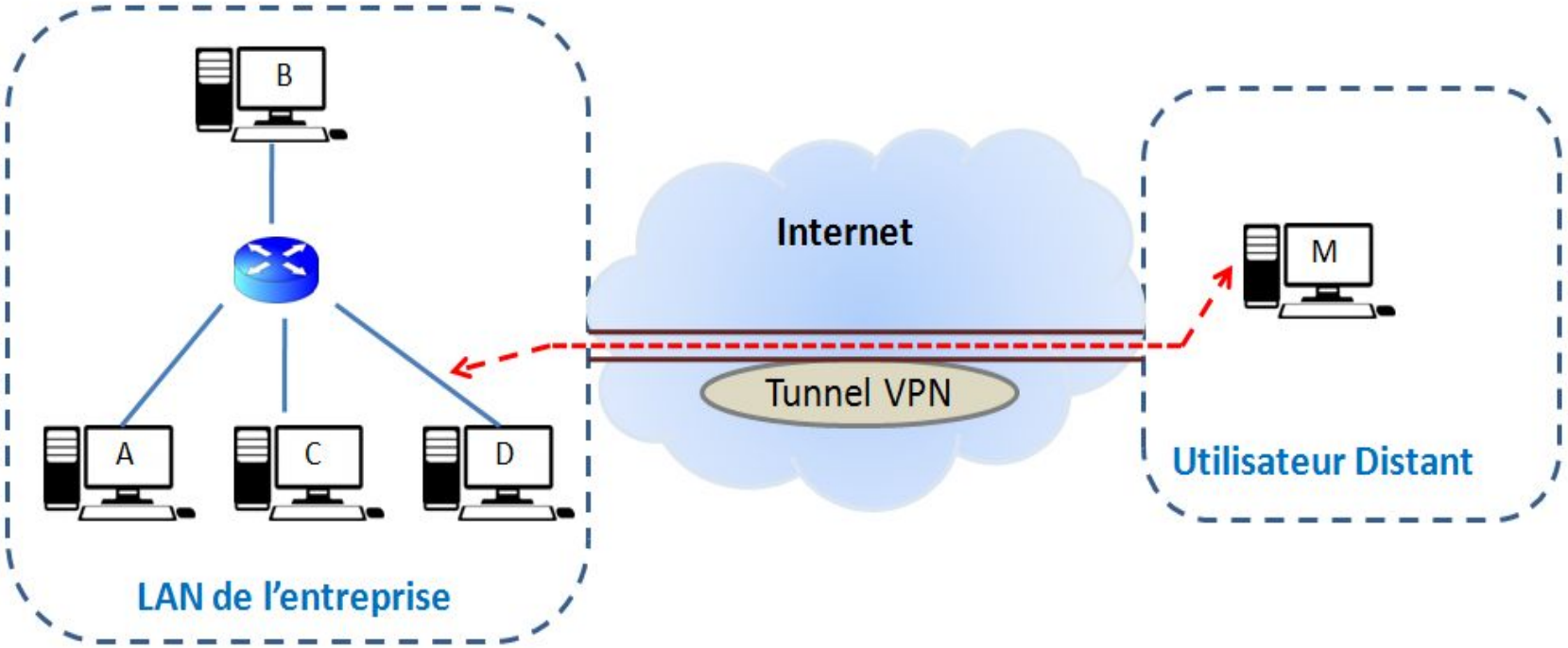
Le VPN est composé de deux mots "**privé**" et "**virtuel**".

- "**Privé**" car il s'agit d'une *communication LAN*.
  Ce qui signifie que les données échangées **ne doivent pas être accessible depuis l'extérieur** (en dehors du VPN).

- "**Virtuel**" car en réalité les réseaux LAN communiquant à l'aide d'un VPN **ne sont pas interconnectés physiquement** (avec des câbles, commutateurs, etc. comme c'est le cas dans un vrai LAN) **mais passent par internet** pour échanger les données.

Réseaux privés virtuels

Afin de rendre un réseau privé "**virtuel**" au milieu d'internet, **un VPN crée** ce qu'on appelle un "***tunnel***".



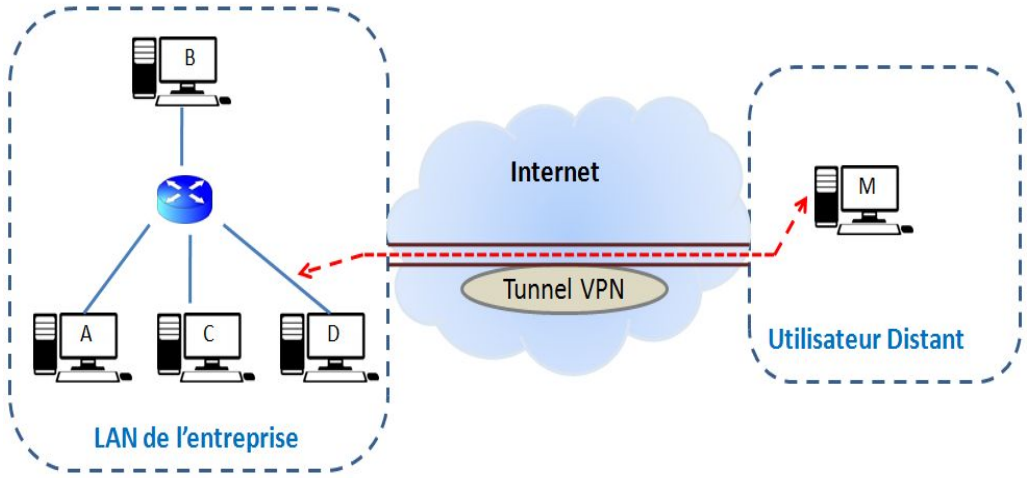
Réseaux privés virtuels

Le **tunnel** VPN doit **pouvoir respecter les points suivants**

- Authentification: seule la **personne autorisée puisse se connecter au VPN** (vérification de l'identité à l'aide d'un code unique par exemple).

- Intégrité: les données transitant le tunnel doivent arrivées à destination tel qu'elles ont été envoyées **sans perte ni modification**.

- Sécurité des données: seule la personne autorisée puisse lire les paquets transitant le tunnel. Les données doivent être protégées par un **cryptage**.



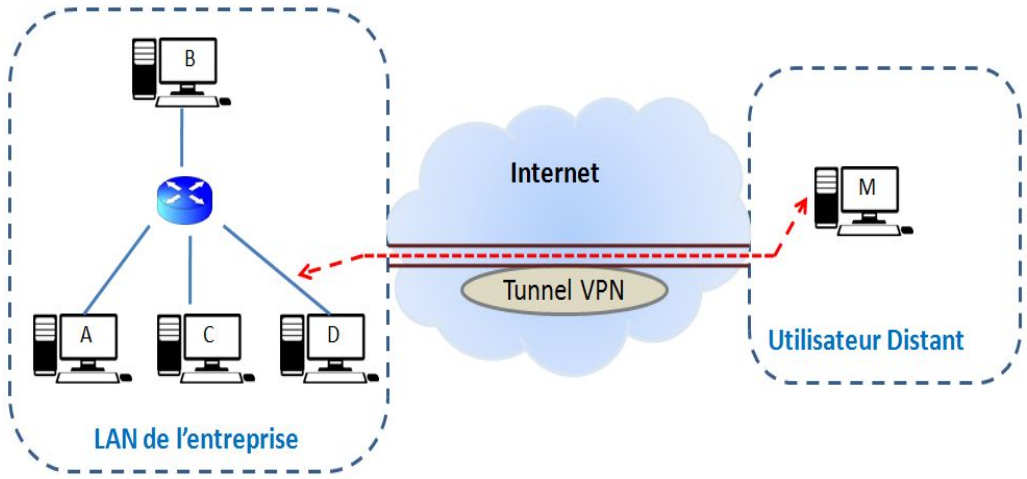
Réseaux privés virtuels

Le tunnel VPN doit pouvoir respecter les points suivants

- Authentification: seule la personne autorisée puisse se connectée au VPN (vérification de l'identité à l'aide d'un code unique par exemple).

- Intégrité: les données transitant le tunnel doivent arrivées à destination tel qu'elles ont été envoyées sans perte ni modification.

- Sécurité des données: seule la personne autorisée puisse lire les paquets transitant le tunnel. Les données doivent être protégées par un cryptage.



En plus des points ci-dessus, un service VPN doit pouvoir gérer les clés de cryptage entre le client et le serveur et doit supporter les protocoles les plus utilisés sur les réseaux publics comme le protocole IP.

Réseaux privés virtuels - Modes d'utilisation d'un VPN

Un réseau privé virtuel peut être utilisé de deux façons

1. **Intranet ou extranet VPN (LAN-to-LAN)**

- Permet de relier **deux réseaux LAN**.
- **Extranet** permet, par exemple, de relier une **entreprise avec ses collaborateurs** ou clients.
- **Intranet** VPN, permet, par exemple, de **relier deux serveurs distants** d'une même entreprise de façon sécurisée.

2. **VPN d'accès (Host-to-LAN)**

- Permet, par exemple, à un **télétravailleur** de se connecter au réseau local de son entreprise à distance
  - Pour travailler,
  - Pour accéder à des données privées,
  - ou pour communiquer avec ses collègues de travail qui à leur tour peuvent être connectés en VPN.
- **Nécessite un code d'accès** pour chaque connexion au VPN.

Réseaux privés virtuels - Principe de fonctionnement d'un VPN (1/4)

1. Le protocole permettant aux données de l'entreprise à transiter un tunnel VPN de bout en bout est appelé "***protocole de tunneling***".

Ce protocole permet de

- faire transiter ces données de **façon cryptée** et
- **assure une transparence** aux utilisateurs qui auront l'impression d'être connectés directement au réseau LAN de l'entreprise
  → **Alors qu'en réalité ils utilisent** une infrastructure d'accès partagée (**internet**).

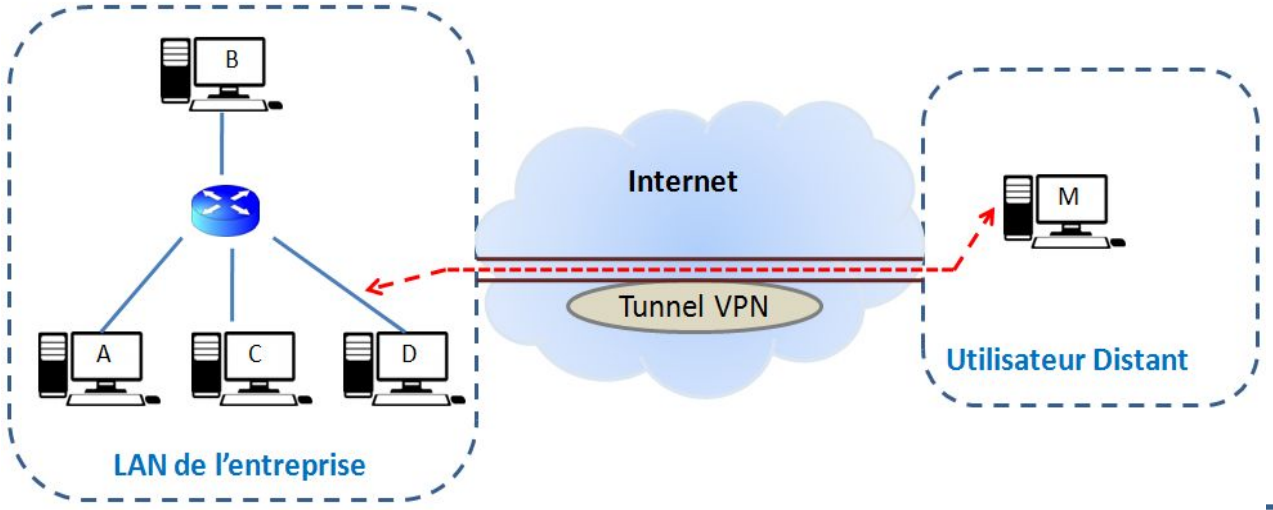
Réseaux privés virtuels - Principe de fonctionnement d'un VPN (2/4)

2. Après avoir identifié la source et la destination, le protocole de tunneling crée un chemin virtuel entre les deux.

3. Le protocole de tunneling encapsule les données en ajoutant une entête, assure la transmission des données et dé-encapsule les données à leurs arrivées à destination.

Réseaux privés virtuels -
Principe de fonctionnement d'un VPN (3/4)

- Au niveau de l'extrémité côté source, les **données** à transporter depuis la machine source **sont insérées dans un paquet** de protocole de "tunnélisation", puis dans un paquet du protocole de transport de données.
- Au niveau de l'extrémité côté destination, les **données sont extraites du protocole** de "tunnélisation" et ensuite **poursuivent leur chemin sous leur forme initiale** afin d'atteindre la destination final.



Réseaux privés virtuels - Principe de fonctionnement d'un VPN (4/4)

4. La configuration se fait au niveau **des routeurs d'entrées et de sorties**, et les paquets avec des adresses **IP privées** sont encapsulées dans des paquets avec des adresses **IPs publiques**.

Réseaux privés virtuels - Avantages des VPNs

Le service VPN présente plusieurs avantages, on cite:

- **Premier** avantage: consiste à assurer une **communication sécurisée et cryptée** entre plusieurs sites.

- **Deuxième** avantage: concerne **la simplicité de son utilisation**.
  En effet, le VPN utilise les circuits des réseaux de télécommunication publics déjà existant.

- **Troisième** avantage: **le coût de son utilisation**.
  Vu que le VPN utilise internet comme mode de transport.
  Ceci évite des coûts supplémentaires pour la création d'une ligne dédiée.

Réseaux privés virtuels - Différents types de VPN

Il existe plusieurs protocoles dit de tunnellisation permettant la création des réseaux VPN.

Les plus connus sont

- **PPTP VPN**
- **Site-to-Site VPN**
- **L2TP VPN**
- **IPsec**
- **SSL**
- **MPLS VPN**
- **Hybrid VPN**

Réseaux privés virtuels - Différents types de VPN

- **PPTP VPN**: **P**oint-to-**P**oint **T**unneling **P**rotocol
  - Old VPN protocol (now insecure, mostly deprecated)
- **Site-to-Site VPN**
  - VPN connecting **two or more networks** (e.g., headquarters ↔ branch)
- **L2TP VPN: L**ayer **2 T**unneling **P**rotocol
  - Tunneling protocol, usually combined with IPsec for security
- **IPsec: I**nternet **P**rotocol **Sec**urity
  - Suite of protocols providing **authentication, integrity, and encryption**
- **SSL**: **S**ecure **S**ockets **L**ayer
  - Cryptographic protocol (today mainly replaced by TLS) used for secure VPN access via browsers
- **MPLS VPN**: **M**ulti-**P**rotocol **L**abel **S**witching **V**irtual **P**rivate **N**etwork
  - Provider-managed VPN using label switching (not encryption-focused)
- **Hybrid VPN**
  - Combination of **multiple VPN technologies** (e.g., MPLS + IPsec)

Réseaux privés virtuels - Différents types de VPN

PPTP, L2TP, IPsec, SSL = tunneling/security technologies

Site-to-Site, MPLS, Hybrid = VPN **architectures or deployment models**

Réseaux privés virtuels -
Protocoles VPN par couche

a) Protocoles de niveau 2 : PPTP, L2TP tous les deux encapsulent les données utiles (payload) dans une trame qui sera transmise à travers Internet.

- Le tunnel est semblable à une session.
- Les deux extrémités du tunnel doivent être d'accord et doivent négocier des variables de configuration, assignation des adresses, paramètres d'encryptions et/ou de compression.
- Un mécanisme de gestion et de maintenance du tunnel.

b) Protocoles de niveau 3 : IPSec encapsule les paquets IP dans un autre paquet IP avant de l'envoyer sur Internet.

- Les variables sont pré-configurées.
- Pas de phase d'entretien de tunnel.

c) Protocoles de niveau 4 : utilise TLS/SSL pour sécuriser les échanges au niveau de la couche Transport.

Réseaux privés virtuels -
Principales différences entre les protocoles VPN

- **Vitesse de la connexion internet :** Plus le protocole de tunneling est puissant et sécurisé (ce qui signifie qu'il utilise des couches de cryptages différentes) plus la connexion est ralentie. Le protocole PPTP est connu par sa vitesse de connexion car il utilise un mécanisme de cryptage pas très performant (128 bits) raison à laquelle il n'est pas conseillé pour des besoins de sécurité.

- **Simplicité de configuration :**

- **Qualité de la sécurité :**

Réseaux privés virtuels -
Principales différences entre les protocoles VPN

- **Vitesse de la connexion internet :** Plus le protocole de tunneling est puissant et sécurisé (ce qui signifie qu'il utilise des couches de cryptages différentes) plus la connexion est ralentie. Le protocole PPTP est connu par sa vitesse de connexion car il utilise un mécanisme de cryptage pas très performant (128 bits) raison à laquelle il n'est pas conseillé pour des besoins de sécurité.

- **Simplicité de configuration :** chaque protocole a son processus de configuration, et certains protocoles sont plus difficile à configurer que d'autres. Les plus facile à configurer sont conseillés aux débutant (le cas du VPN PPTP). Tandis que les VPNs comme OpenVPN et IPSec demandent plus d'expertises pour être parfaitement personnalisé pour un utilisateur donné. Tous les services VPN possèdent des paramètres par défaut.

- **Qualité de la sécurité :**

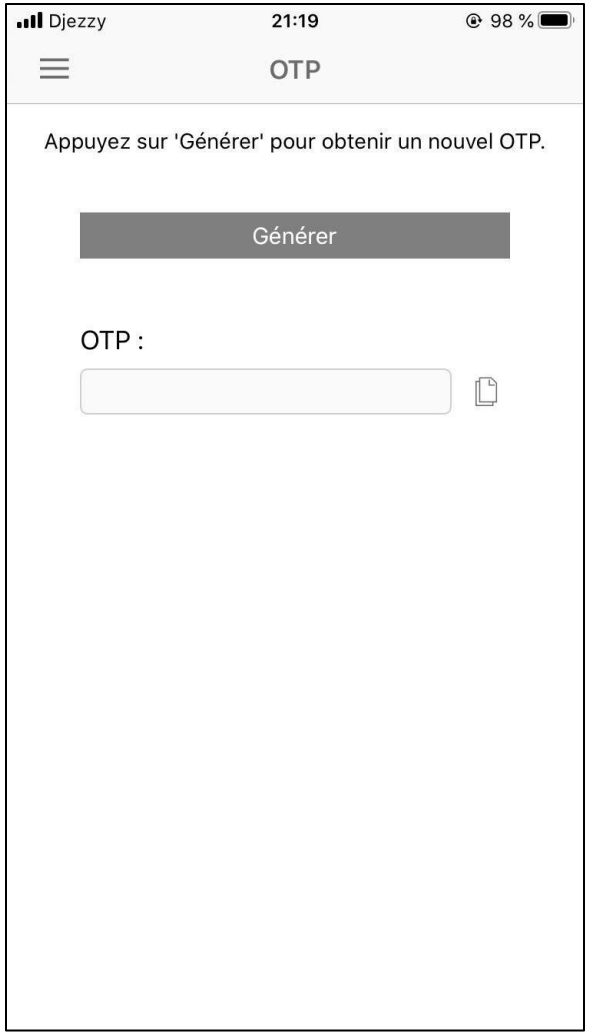
Réseaux privés virtuels -
Principales différences entre les protocoles VPN

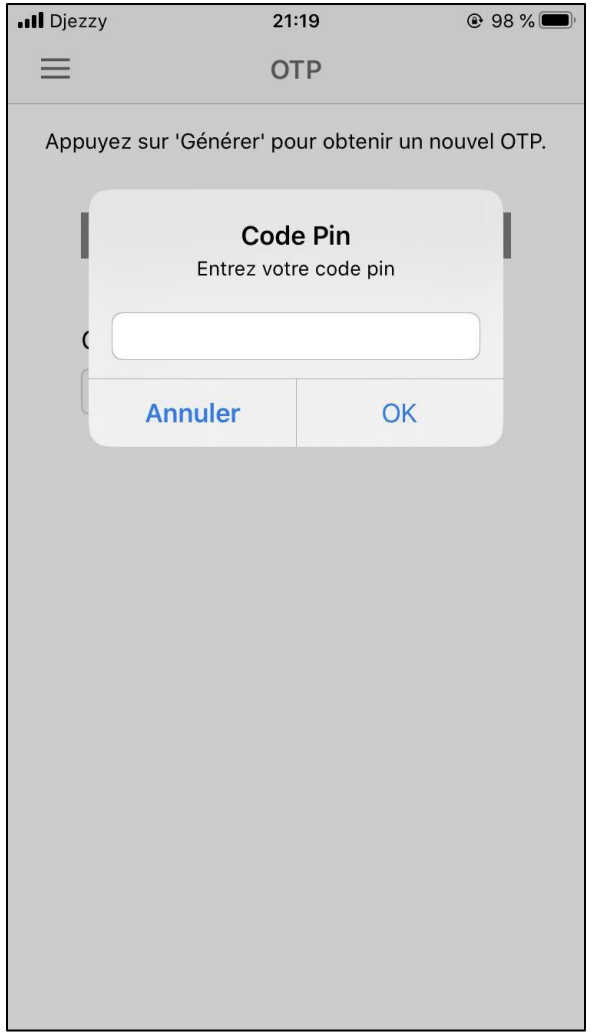
- **Vitesse de la connexion internet :** Plus le protocole de tunneling est puissant et sécurisé (ce qui signifie qu'il utilise des couches de cryptages différentes) plus la connexion est ralentie. Le protocole PPTP est connu par sa vitesse de connexion car il utilise un mécanisme de cryptage pas très performant (128 bits) raison à laquelle il n'est pas conseillé pour des besoins de sécurité.

- **Simplicité de configuration :** chaque protocole a son processus de configuration, et certains protocoles sont plus difficile à configurer que d'autres. Les plus facile à configurer sont conseillés aux débutant (le cas du VPN PPTP). Tandis que les VPNs comme OpenVPN et IPSec demandent plus d'expertises pour être parfaitement personnalisé pour un utilisateur donné. Tous les services VPN possèdent des paramètres par défaut.

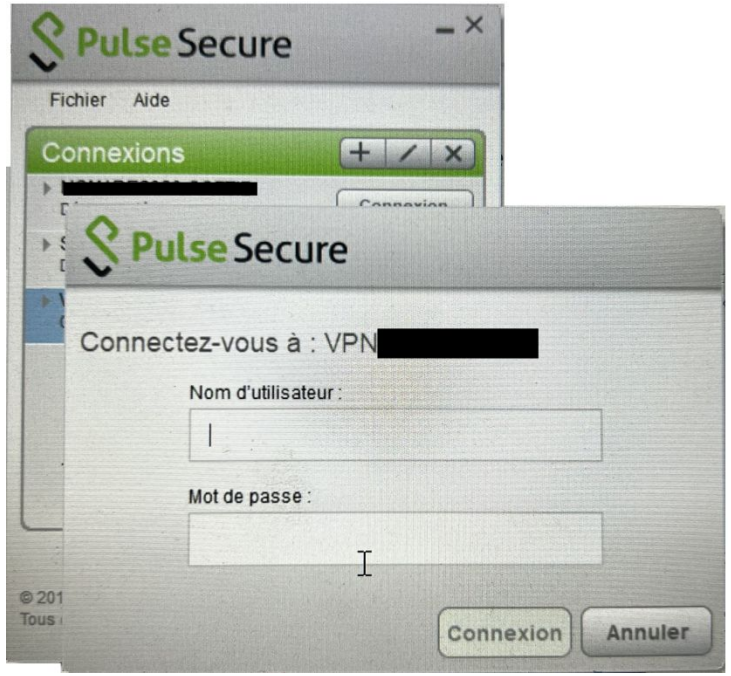
- **Qualité de la sécurité :** C'est le point le plus important dans un service VPN. La sécurité assurée par les protocoles de tunneling varie d'un protocole à un autre suivant l'algorithme ou la méthode de chiffrement utilisé. L'exemple de PPTP est le meilleur exemple. Ce protocole, pourtant, considéré comme sécurisé à ses débuts aujourd'hui ce n'est plus le cas.

Exemple avec l’application SSOX Pro

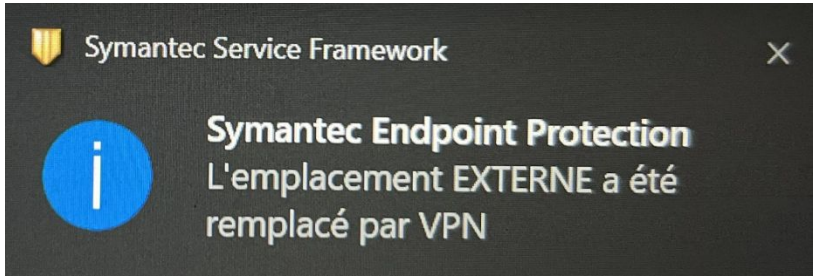




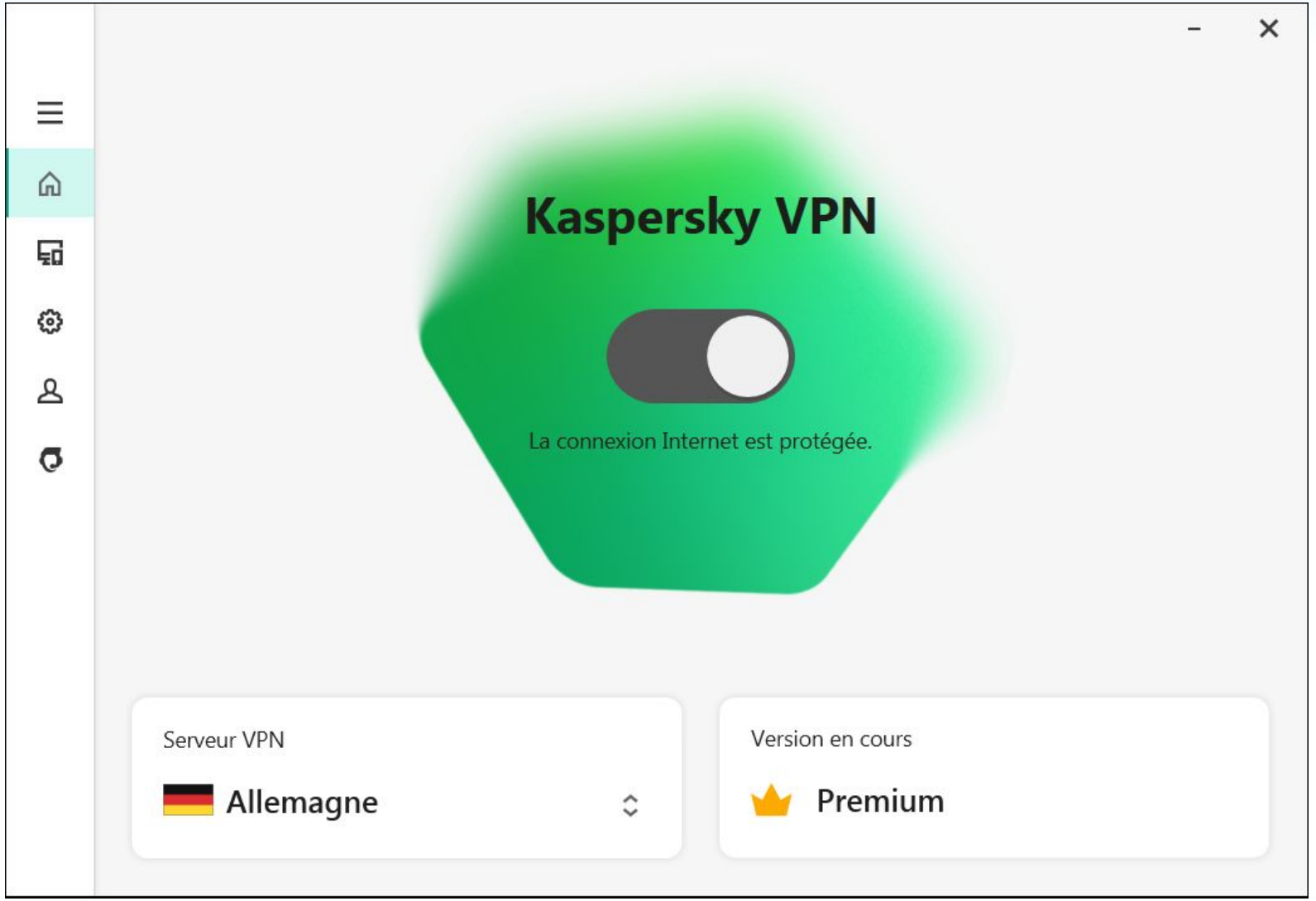
Exemple Pulse Secure



Pulse Secure



Exemple avec Kaspersky VPN



Conclusion

Choisir le meilleur VPN n'est pas une tâche facile.

Il faut, avant tout, étudier **le besoin de votre client** en termes de

- architecture réseau
- coût
- sécurité
- rapidité

Est-ce que le besoin tant vers un VPN LAN-to-LAN ou Host-to-LAN ?

Conclusion

Choisir le meilleur VPN n'est pas une tâche facile.

Il faut, avant tout, étudier **le besoin de votre client** en termes de

- architecture réseau,
- coût,
- sécurité
- rapidité,

Est-ce que le besoin tant vers un VPN LAN-to-LAN ou Host-to-LAN ?

Si on prend l'exemple de **PPTP**, la **vitesse de connexion est excellente** et la **configuration est très simple**, cependant la **sécurité des données n'est pas garantie**.

Il faut savoir que **plus le protocole choisi est puissant et sécurisé**, **plus la connexion est ralentie**.