Virtual Private Network

Question: Comment une succursale d'une entreprise peut-elle accéder en sécurité aux données situées sur un serveur de la maison mère distante de plusieurs milliers de kilomètres ?

- **Une solution**: VPN (Virtual Private Network)

- Accès au réseau local (d'entreprise) à distance et de façon sécurisée pour les **travailleurs nomades.**

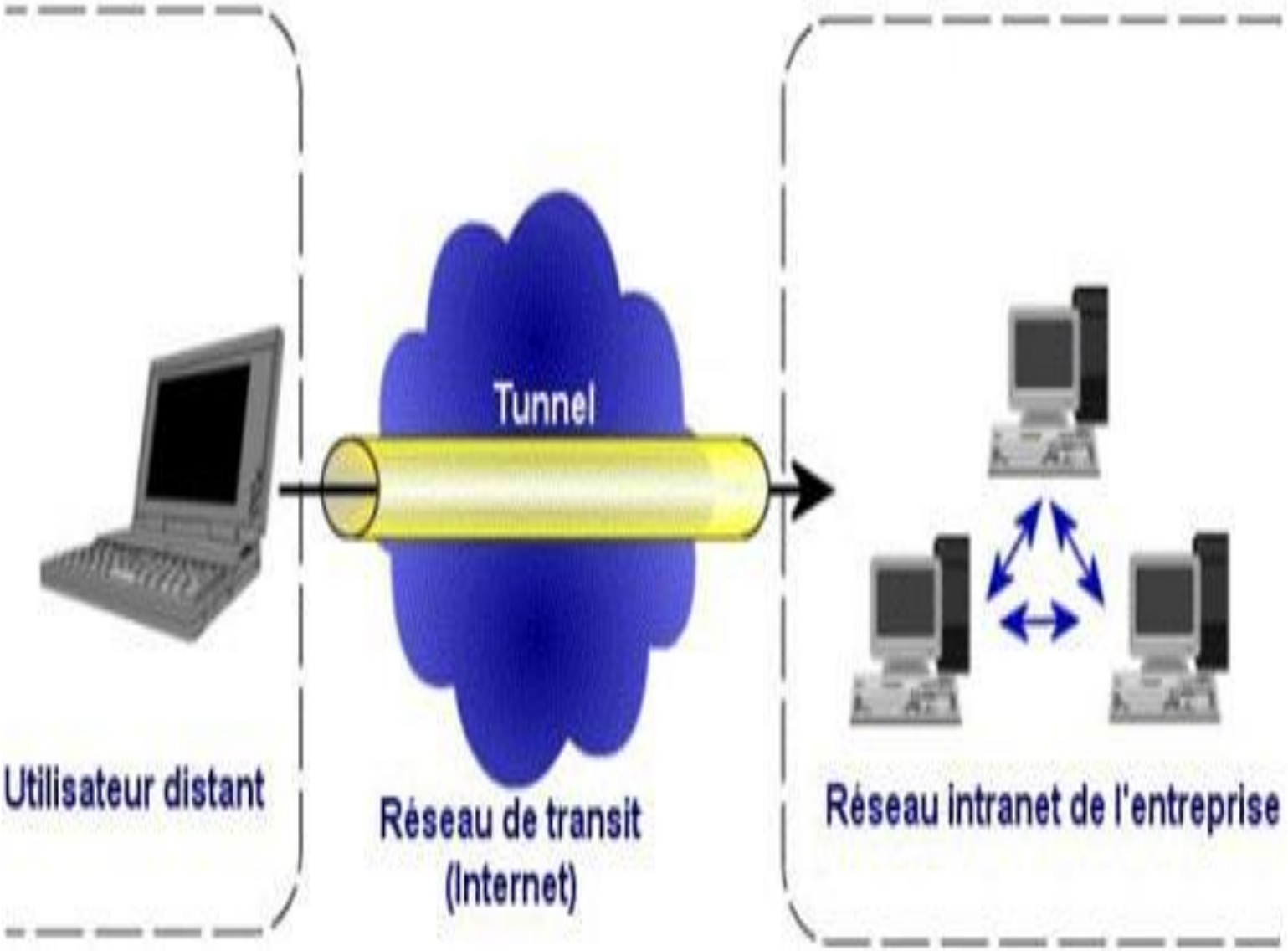
- Partage de fichiers sécurisés
- ...

Principe:

Un réseau VPN repose sur un protocole appelé "protocole de **tunneling**".

• Ce protocole permet de faire circuler les informations de l'entreprise de façon **cryptée** d'un bout à l'autre du tunnel.

• Les utilisateurs ont l'impression de se connecter directement sur le réseau de leur entreprise


Tunnel
Utilisateur distant
Réseau de transit
(Internet)
Réseau intranet de l'entreprise

Le principe de **tunneling** consiste à construire un chemin virtuel après avoir identifié l'émetteur et le destinataire.

- La source **chiffre** les données et les achemine en empruntant ce chemin virtuel.

Afin d'assurer un accès aisé et peu coûteux aux intranets ou aux extranets d'entreprise, les réseaux privés virtuels d'accès simulent un réseau privé, alors qu'ils utilisent en réalité une infrastructure d'accès partagée, comme Internet.

Les données à transmettre peuvent être prises en charge par un protocole différent d'IP.

Dans ce cas, le protocole de tunneling **encapsule** les données en ajoutant une en-tête.

Le tunneling est l'ensemble des processus d'encapsulation, de transmission et de désencapsulation.

Fonctionnalités des VPN

Le VPN d'accès est utilisé pour permettre à des utilisateurs **itinérants** d'accéder au réseau privé.

• L'utilisateur se sert d'une connexion Internet pour établir la connexion VPN. Il existe deux cas:

1. L'utilisateur demande au fournisseur d'accès de lui établir une connexion **cryptée** vers le serveur distant : il communique avec le **NAS** (Network Access Server) du fournisseur d'accès et c'est le **NAS** qui établit la connexion **cryptée**.

2. L'utilisateur possède son propre logiciel client pour le VPN auquel cas il établit directement la communication de manière cryptée vers le réseau de l'entreprise.

Les deux méthodes possèdent chacune leurs avantages et leurs inconvénients :

- La première permet à l'utilisateur de communiquer sur plusieurs réseaux en créant plusieurs tunnels:

- **Nécessité d’un fournisseur d'accès proposant un NAS compatible avec la solution VPN choisie par l'entreprise.**
- **Demande de connexion par le NAS n'est pas cryptée (problèmes de sécurité).**

Pour la deuxième méthode:

Le problème de sécurité disparaît puisque l'intégralité des informations sera cryptée dès l'établissement de la connexion.

Mais:

la solution nécessite que chaque client transporte avec lui le logiciel, lui permettant d'établir une communication cryptée.

Pour pallier ce problème, mise en place de VPN à base de **SSL**

Quelle que soit la méthode de connexion choisie, le VPN impose d'avoir une authentification forte des utilisateurs.

Cette authentification peut se faire par:

- une vérification "login / mot de passe",
- un algorithme dit "Tokens sécurisés"

(utilisation de mots de passe aléatoires)

- ou certificats numériques.

Bilan des caractéristiques fondamentales d'un VPN

Un système de VPN doit pouvoir mettre en oeuvre les fonctionnalités suivantes :

- **Authentification d'utilisateurs**.

  Seuls les utilisateurs autorisés doivent pouvoir s'identifier sur le réseau virtuel.

  De plus, un historique des connexions et des actions effectuées sur le réseau doit être conservé.

- **Gestion d'adresses**. Chaque client sur le réseau doit avoir une adresse privée. Cette adresse privée doit rester confidentielle.

Bilan des caractéristiques (suite)

•**Cryptage des données**. Lors de leurs transports sur le réseau public les données doivent être protégées par un cryptage efficace.

•**Gestion de clés**. Les clés de cryptage pour le client et le serveur doivent pouvoir être générées et régénérées.

•**Prise en charge multiprotocole**. La solution VPN doit supporter les protocoles les plus utilisés sur les réseaux publics en particulier IP.

Protocoles utilisés pour réaliser une connexion VPN

Les protocoles étudiés sont deux catégories:

✓Les protocoles de niveau 2 comme PPTP et L2TP

✓Les protocoles de niveau 3 comme IPSEC ou MPLS.

•Il existe **3** protocoles de niveau 2 permettant de réaliser des VPN **PPTP** (de Microsoft), **L2F** (développé par CISCO) & **L2TP**. **L2F ayant aujourd'hui quasiment disparu**.

• PPTP aurait sans doute lui aussi disparu Microsoft l'intègre à ses systèmes d'exploitation Windows.

• L2TP est une évolution de PPTP et de L2F, reprenant les avantages des deux protocoles.

PROTOCOLE PPP

PPP (Point to Point Protocol) est un protocole de transfère des données sur un lien synchrone ou asynchrone.

•Il garantit **l'ordre d'arrivée** des paquets.

•Il **encapsule** les paquets IP des trames PPP, puis transmet ces paquets encapsulés au travers de la liaison point à point.

•PPP est employé généralement entre un client d'accès à distance et un serveur d'accès réseau (NAS).

PROTOCOLE PPP

- **Le protocole PPP n'est pas un protocole permettant l'établissement d'un VPN**

Mais

- **Il est très souvent utilisé pour transférer les informations au travers d'un VPN.**

PROTOCOLE PPTP

PPTP est un protocole qui utilise une connexion PPP à travers un réseau IP en créant un VPN.

• PPTP est une solution très employée dans les produits VPN commerciaux à cause de son intégration au sein des systèmes d'exploitation Windows.

• PPTP est un protocole de niveau 2 qui permet l'**encryptage** des données ainsi que leur **compression**.

• Un nouveau client doit pourvoir se connecter facilement au réseau et recevoir une adresse.

PROTOCOLE PPTP

• L'**authentification** se fait grâce au protocole **Ms-Chap** de Microsoft qui, après la **cryptanalyse** de sa version 1, a révélé publiquement des failles importantes.

•Microsoft a corrigé ces défaillances et propose aujourd'hui une version 2 de **Ms-Chap** plus sûre.

•La partie chiffrement des données s'effectue grâce au protocole **MPPE** (Microsoft Point-to-Point Encryption).

- Microsoft a mis au point une version spécifique de CHAP, *MS-CHAP* (***Microsoft Challenge Handshake Authentication Protocol*** version 1 améliorant la sécurité.

- CHAP implique que l'ensemble des mots de passe des utilisateurs soient stockés en clair sur le serveur:

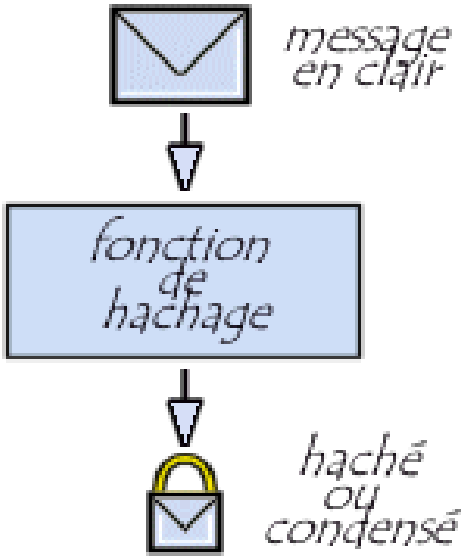
d'où **vulnérabilité potentielle**.

MS-CHAP propose une fonction de **hachage** propriétaire permettant de stocker un **hash** intermédiaire du mot de passe sur le serveur:

✓ Le protocole MS-CHAP-v1 souffre de failles de sécurité liées à des faiblesses de la fonction de hachage propriétaire.

- Une **fonction de hachage** (*fonction de condensation*) est une fonction permettant d'obtenir un condensé (*haché* ou en anglais *message digest*) d'un texte, i.e une suite de caractères assez courte représentant le texte qu'il condense.

- La fonction de hachage doit être telle qu'elle associe un et un seul haché à un texte en clair.



Le principe du protocole **PPTP** est de créer des paquets sous le protocole **PPP** et de les encapsuler dans des datagrammes IP.

Le tunnel PPTP se caractérise par:

- **une initialisation du client,**
- **une connexion de contrôle entre le client et le serveur,**
- **la clôture du tunnel par le serveur.**

- Lors de l'établissement de la connexion, le client effectue d'abord une connexion avec son fournisseur d'accès Internet.

- Cette première connexion établie une connexion de type **PPP** et permet de faire circuler des données sur Internet.

- Une deuxième connexion dial-up est établie.
- Elle permet d'encapsuler les paquets PPP dans des **datagrammes** IP.

Cette deuxième connexion forme le tunnel **PPTP**:

- Tout trafic client conçu pour Internet emprunte la connexion physique normale
- Le trafic conçu pour le réseau privé distant passe par la connexion virtuelle de PPTP.

- Le protocole PPTP un protocole de niveau 2 qui encapsule des trames PPP dans des datagrammes IP afin de les transférer sur un réseau IP.

- PPTP permet le **chiffrement** des données PPP encapsulées mais aussi leur **compression**.

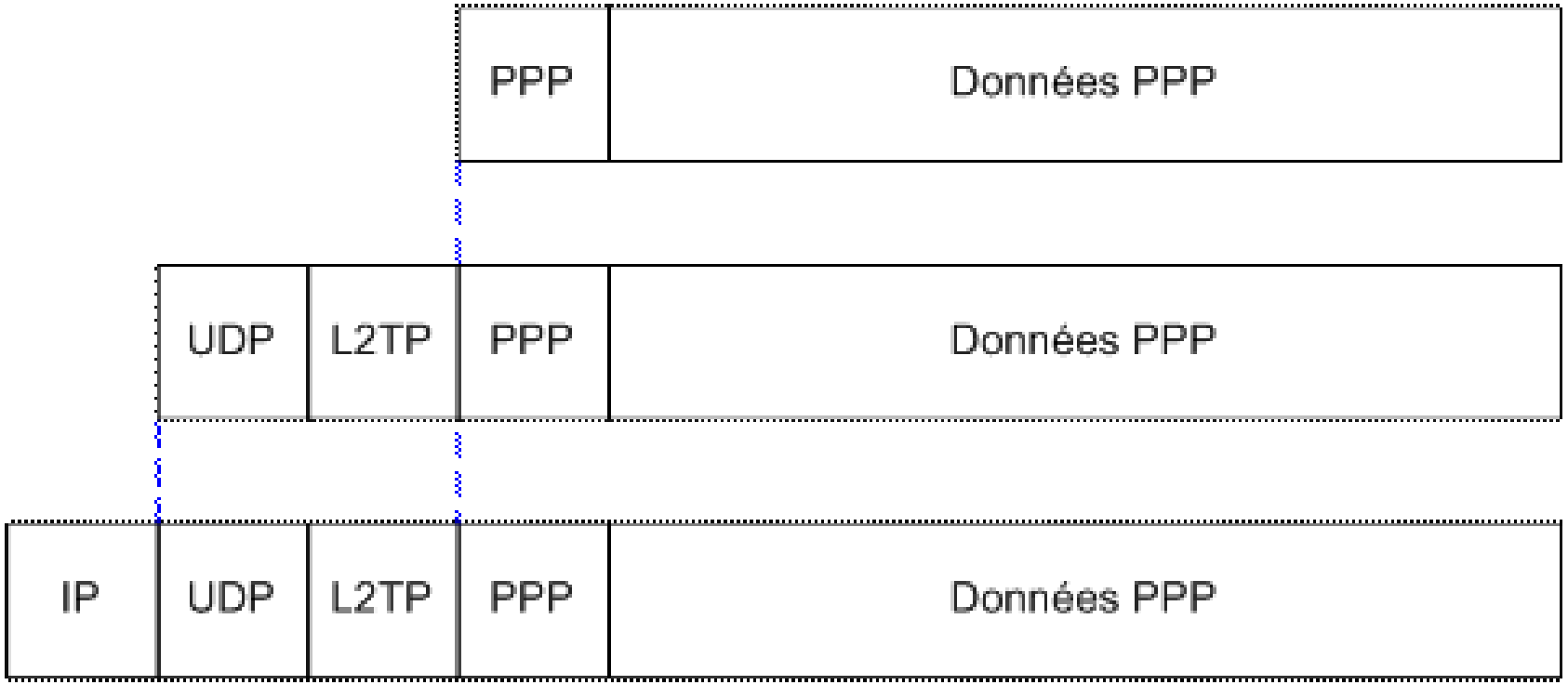
Protocole L2TP (Layer Two Tunneling Protocol)

- Le protocole L2TP (Layer Two Tunneling Protocol) est un protocole de tunneling

- Contrairement à PPTP, L2TP dans Windows 2000 n'utilise pas MPPE (Microsoft Point-to-Point Encryption) pour crypter les datagrammes PPP.

- L2TP s'appuie sur les services de cryptage de la sécurité du protocole Internet (**IPSec**). La combinaison de L2TP et IPSec est connue sous la désignation " L2TP sur IPSec ".

Mode de fonctionnement du protocole L2TP



Le protocole L2TP transporte des trames PPP dans des paquets IP.

Le protocole UDP est utilisé pour envoyer les trames PPP au sein de trames L2TP.

Ipsec

IPSec est une ensemble de protocoles développés par l'IETF (**Internet Engineering Task Force**) qui a pour vocation d'établir des canaux communications sécurisés garantissant l'**intégrité** et la **confidentialité** des données véhiculées au niveau de la couche IP.

- IPSec est largement utilisé par les équipements VPN en entreprise.

  Certaines configurations IPSec qui utilisent notamment l'ESP (Encapsulating Security Payload) ou AH (Authentication Header) seraient **vulnérables** à une attaque permettant d'intercepter les données en clair.

Un dogme s'effondre

La confidentialité des données véhiculées à travers un tunnel IPSec est remise en question.

- D'après le **NISCC** (Nationnal Infrastructure Security Coordination Centre) , 1 vulnérabilité a pu être démontrée en laboratoire au prix d'un effort *"modéré"*.

  Bien sûr, l'attaque requiert que l'assaillant puisse intercepter les paquets IPSec sur le réseau.

Mise en place d'un VPN sous windows

Windows XP permet de gérer nativement des réseaux privés virtuels de petite taille, convenant pour des réseaux de petites entreprises ou familiaux (appelés *SOHO*, *Small Office/Home Office*).

Pour mettre en place un réseau privé virtuel:

- installer au niveau du réseau local un serveur d'accès distant (serveur VPN) accessible depuis Internet

- paramétrer chaque client pour lui permettre de s'y connecter.