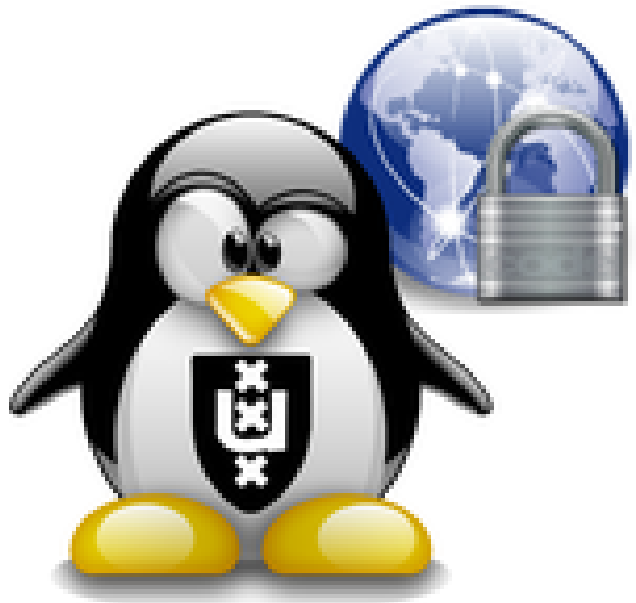
Virtual Private Network (VPN)

Éric BERTHOMIER
eric.berthomier@free.fr

16 mars 2022



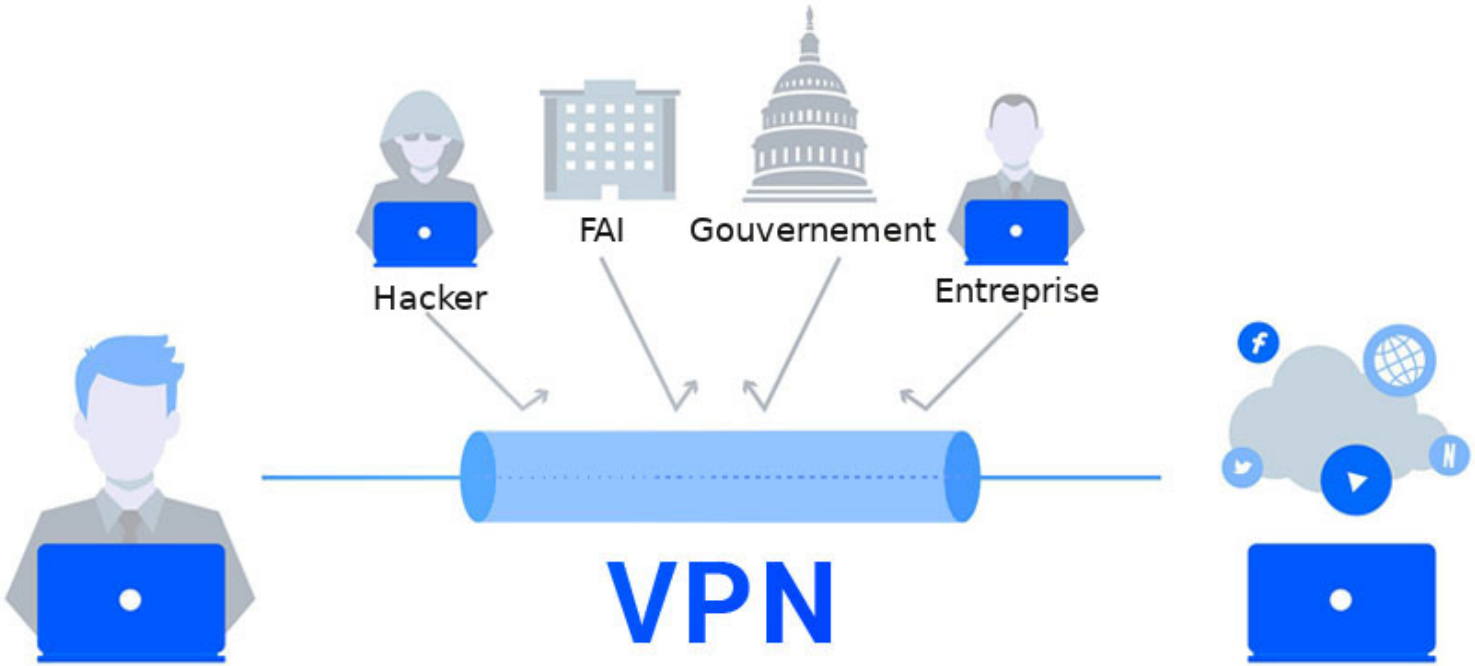
Version 1.0 - Version Stagiaire

Définition

VPN signifie Virtual Private Network ou Réseau Privé Virtuel (RPV).

Définition

VPN signifie Virtual Private Network ou Réseau Privé Virtuel (RPV).
Technologie permettant denvoyer des données entre des ordinateurs appartenant à des sites distants, par lintermédiaire dun inter-réseau public de la même manière que sil sagissait dune liaison privée point à point.

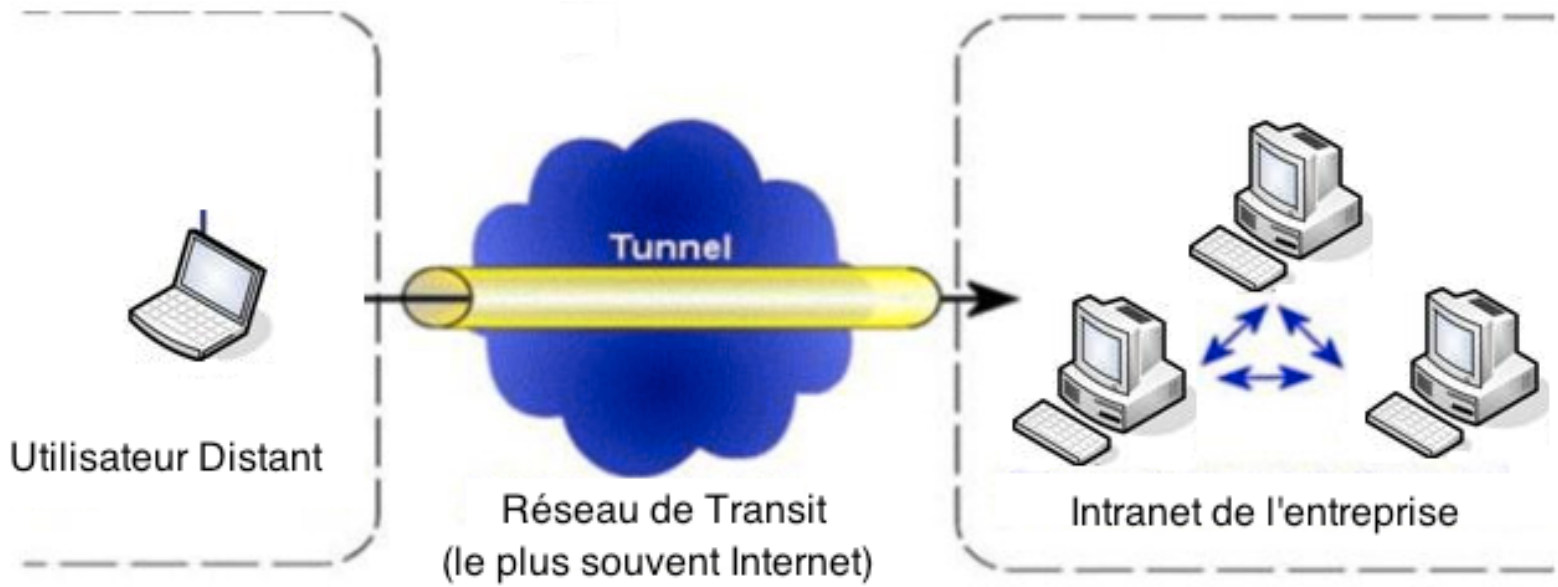


VPN d'accès

Accès distant permettant de connecter un ordinateur à un réseau privé.

VPN d'accès

Accès distant permettant de connecter un ordinateur à un réseau privé.
L'exemple type est une connexion VPN entre un télétravailleur et l'intranet de son entreprise.

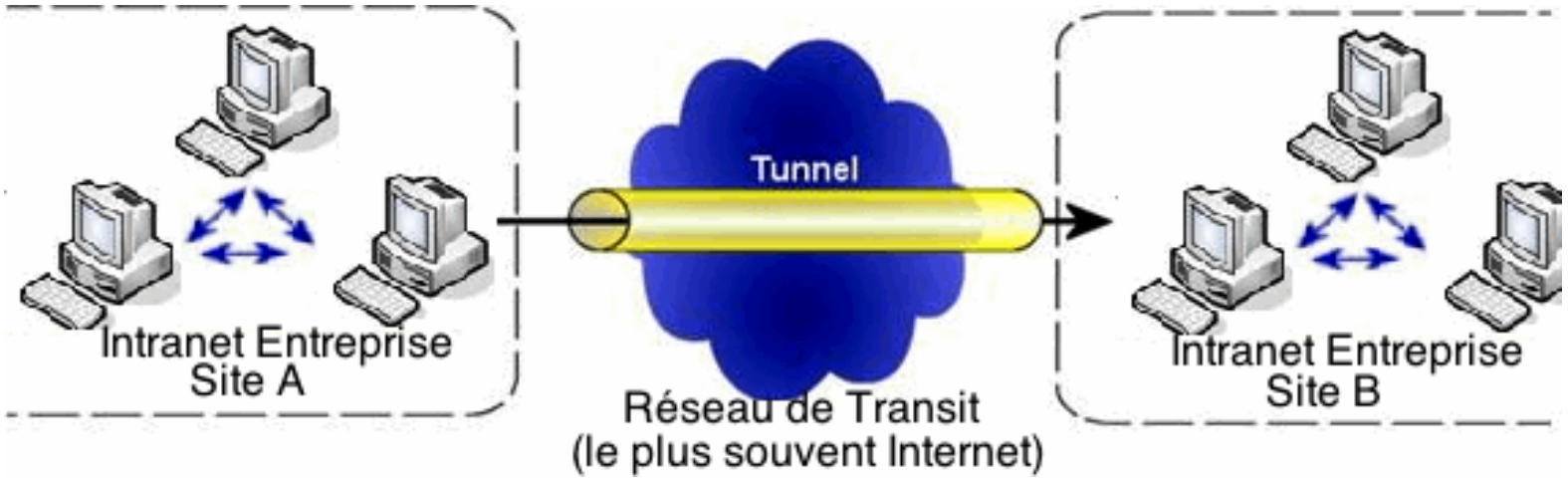


Intranet VPN

Connexion VPN routeur à routeur reliant deux portions de réseau privé éloignées mais appartenant à la même entreprise.

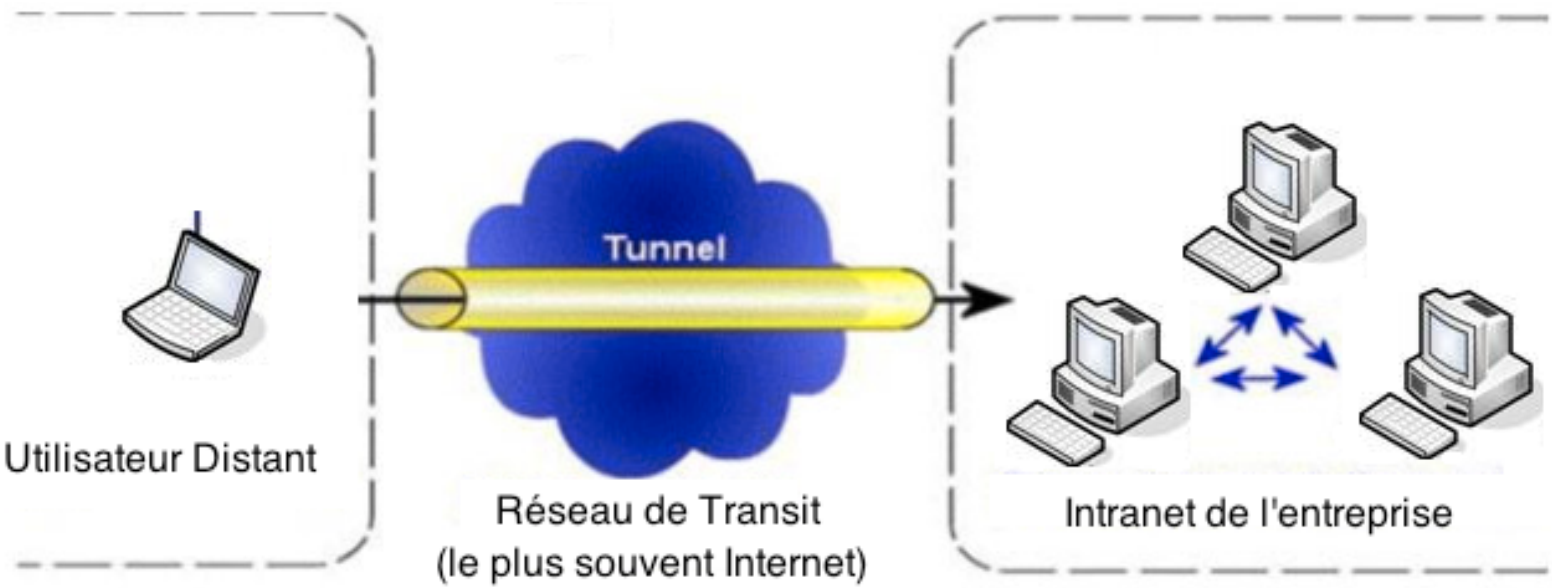
Intranet VPN

Connexion VPN routeur à routeur reliant deux portions de réseau privé éloignées mais appartenant à la même entreprise.
L'exemple type est une connexion VPN entre le siège d'une société et une de ses agences.

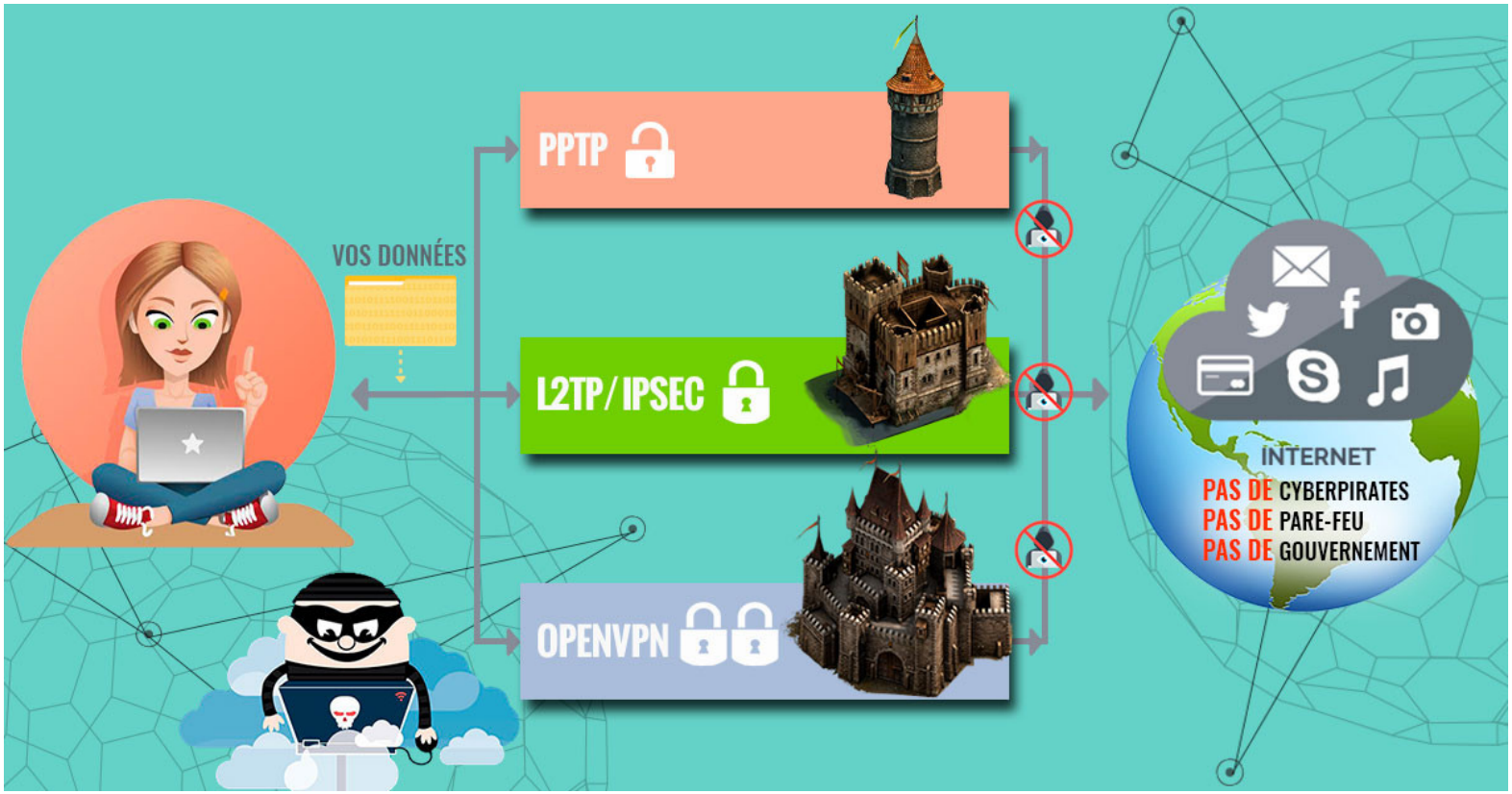


Extranet VPN

Connexion VPN routeur à routeur reliant les réseaux privés de deux entreprises entretenant des rapports commerciaux (client et fournisseur).



Comprendre le VPN



Comprendre le VPN

1. PPTP, protocole de tunnel point-à-point, est un protocole d'encapsulation PPP sur IP conçu par Microsoft.

Comprendre le VPN

1. PPTP, protocole de tunnel point-à-point, est un protocole d'encapsulation PPP sur IP conçu par Microsoft.
2. L2TP : Layer 2 Tunneling Protocol signifie protocole de tunnellisation de niveau 2.

Comprendre le VPN

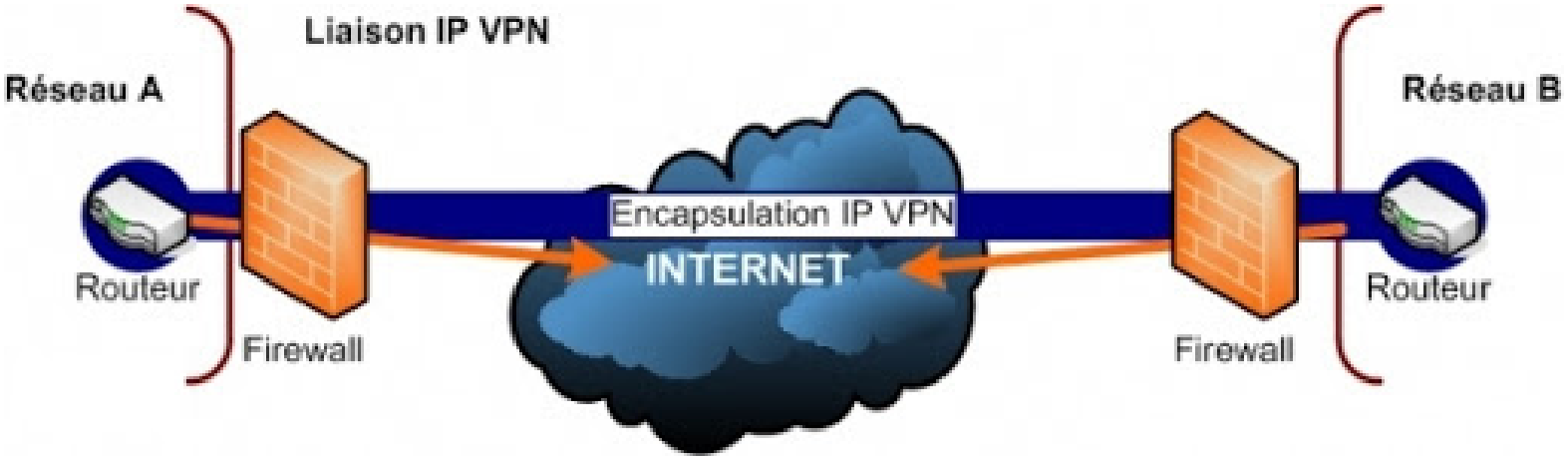
1. PPTP, protocole de tunnel point-à-point, est un protocole d'encapsulation PPP sur IP conçu par Microsoft.
2. L2TP : Layer 2 Tunneling Protocol signifie protocole de tunnellisation de niveau 2.
3. IPsec : Ensemble de protocoles utilisant des algorithmes permettant le transport de données sécurisées sur un réseau IP. Il opère au niveau de la couche réseau (couche 3 du modèle OSI).

Comprendre le VPN

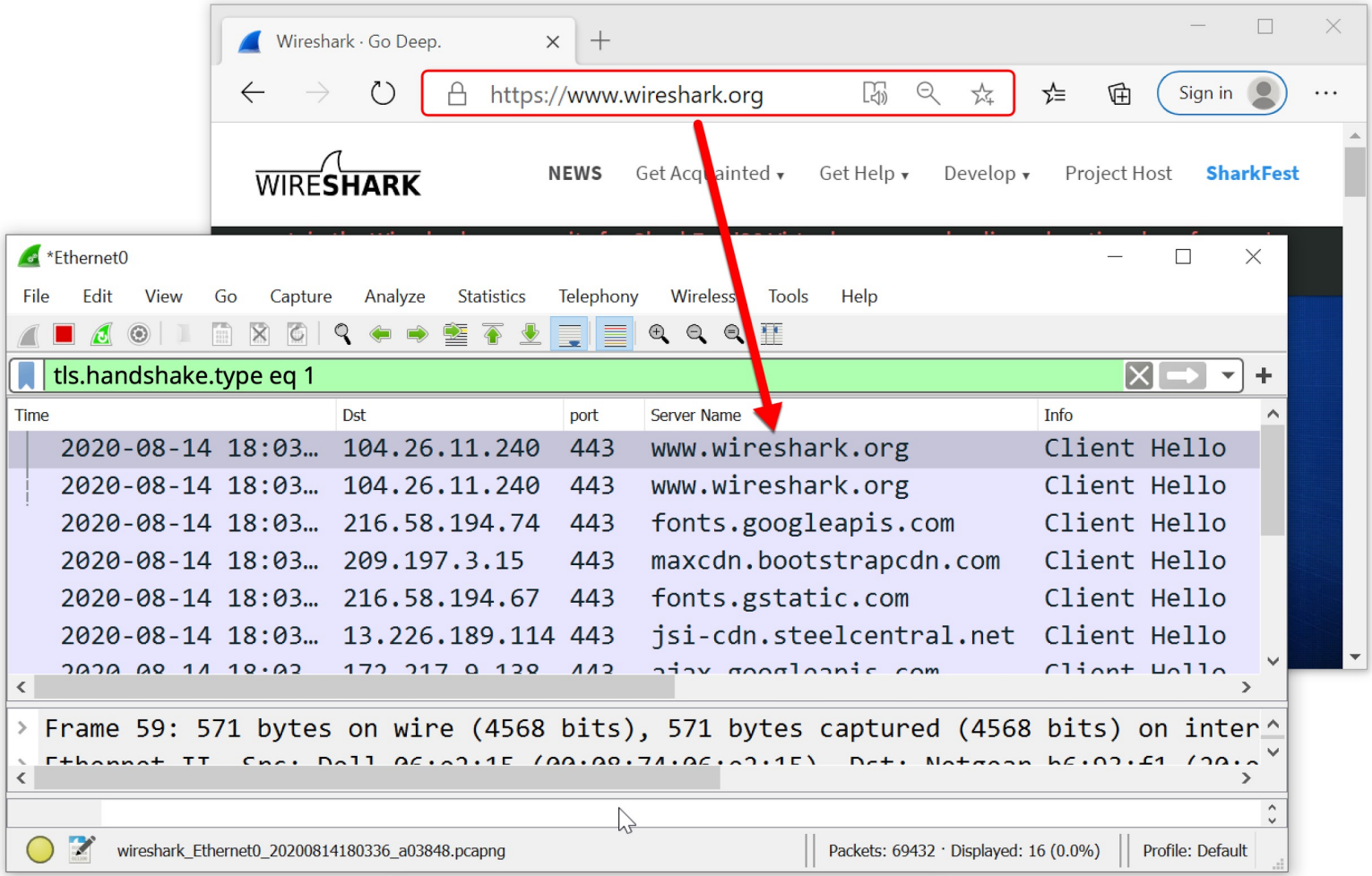
1. PPTP, protocole de tunnel point-à-point, est un protocole d'encapsulation PPP sur IP conçu par Microsoft.
2. L2TP : Layer 2 Tunneling Protocol signifie protocole de tunnellisation de niveau 2.
3. IPsec : Ensemble de protocoles utilisant des algorithmes permettant le transport de données sécurisées sur un réseau IP. Il opère au niveau de la couche réseau (couche 3 du modèle OSI).
4. OpenVPN : OpenVPN permet à des pairs de s'authentifier entre eux à l'aide d'une clé privée partagée à l'avance, de certificats électroniques ou de couples de noms d'utilisateur/mot de passe. Il utilise de manière intensive la bibliothèque d'authentification OpenSSL ainsi que le protocole SSLv3/TLSv1 (Transport Layer Security).

Fondamentaux réseaux

Fondamentaux VPN



Démonstration : TLS



Avantages(1/2)

- Cachez votre trafic de votre FAI, qui ne verra que le trafic crypté vers/depuis le VPN. Ainsi, votre FAI ne peut pas vendre vos données, injecter des publicités ou ralentir en fonction du type de trafic ou de la source de trafic.

Avantages(1/2)

- Cachez votre trafic de votre FAI, qui ne verra que le trafic crypté vers/depuis le VPN. Ainsi, votre FAI ne peut pas vendre vos données, injecter des publicités ou ralentir en fonction du type de trafic ou de la source de trafic.
- Ajoutez une couche supplémentaire de cryptage à votre trafică; protège contre les menaces sur le LAN ou le Wi-Fi.

Avantages(1/2)

- Cachez votre trafic de votre FAI, qui ne verra que le trafic crypté vers/depuis le VPN. Ainsi, votre FAI ne peut pas vendre vos données, injecter des publicités ou ralentir en fonction du type de trafic ou de la source de trafic.
- Ajoutez une couche supplémentaire de cryptage à votre trafică; protège contre les menaces sur le LAN ou le Wi-Fi.
- En utilisant le DNS du VPN, vous obtenez un tunnel sécurisé vers le DNS et votre FAI ne peut pas voir votre trafic DNS.

Avantages(1/2)

- Cachez votre trafic de votre FAI, qui ne verra que le trafic crypté vers/depuis le VPN. Ainsi, votre FAI ne peut pas vendre vos données, injecter des publicités ou ralentir en fonction du type de trafic ou de la source de trafic.
- Ajoutez une couche supplémentaire de cryptage à votre trafică; protège contre les menaces sur le LAN ou le Wi-Fi.
- En utilisant le DNS du VPN, vous obtenez un tunnel sécurisé vers le DNS et votre FAI ne peut pas voir votre trafic DNS.
- Les sites Web et les espions verront l'adresse IP du serveur VPN, pas votre adresse IP personnelle.

Avantages(1/2)

- Cachez votre trafic de votre FAI, qui ne verra que le trafic crypté vers/depuis le VPN. Ainsi, votre FAI ne peut pas vendre vos données, injecter des publicités ou ralentir en fonction du type de trafic ou de la source de trafic.
- Ajoutez une couche supplémentaire de cryptage à votre trafică; protège contre les menaces sur le LAN ou le Wi-Fi.
- En utilisant le DNS du VPN, vous obtenez un tunnel sécurisé vers le DNS et votre FAI ne peut pas voir votre trafic DNS.
- Les sites Web et les espions verront l'adresse IP du serveur VPN, pas votre adresse IP personnelle.
- Mélangez votre trafic avec des centaines ou des milliers d'autres utilisateurs utilisant le même serveur VPN.

Avantages(1/2)

- Cachez votre trafic de votre FAI, qui ne verra que le trafic crypté vers/depuis le VPN. Ainsi, votre FAI ne peut pas vendre vos données, injecter des publicités ou ralentir en fonction du type de trafic ou de la source de trafic.
- Ajoutez une couche supplémentaire de cryptage à votre trafică; protège contre les menaces sur le LAN ou le Wi-Fi.
- En utilisant le DNS du VPN, vous obtenez un tunnel sécurisé vers le DNS et votre FAI ne peut pas voir votre trafic DNS.
- Les sites Web et les espions verront l'adresse IP du serveur VPN, pas votre adresse IP personnelle.
- Mélangez votre trafic avec des centaines ou des milliers d'autres utilisateurs utilisant le même serveur VPN.
- Éliminez le blocage géographique.

Avantages(1/2)

- Cachez votre trafic de votre FAI, qui ne verra que le trafic crypté vers/depuis le VPN. Ainsi, votre FAI ne peut pas vendre vos données, injecter des publicités ou ralentir en fonction du type de trafic ou de la source de trafic.
- Ajoutez une couche supplémentaire de cryptage à votre trafică; protège contre les menaces sur le LAN ou le Wi-Fi.
- En utilisant le DNS du VPN, vous obtenez un tunnel sécurisé vers le DNS et votre FAI ne peut pas voir votre trafic DNS.
- Les sites Web et les espions verront l'adresse IP du serveur VPN, pas votre adresse IP personnelle.
- Mélangez votre trafic avec des centaines ou des milliers d'autres utilisateurs utilisant le même serveur VPN.
- Éliminez le blocage géographique.
- Éliminez le suivi de localisation, lorsqu'un site souhaite associer votre adresse IP à un emplacement physique.

Avantages (2/2)

- Flexibilité : vous pouvez activer et désactiver le VPN, ou changer de serveur VPN, comme vous le souhaitez.

Avantages (2/2)

- Flexibilité : vous pouvez activer et désactiver le VPN, ou changer de serveur VPN, comme vous le souhaitez.
- Ajoutez plusieurs juridictions/pays, si quelqu'un veut vous poursuivre pour infraction à la protection des droits d'auteur.

Avantages (2/2)

- Flexibilité : vous pouvez activer et désactiver le VPN, ou changer de serveur VPN, comme vous le souhaitez.
- Ajoutez plusieurs juridictions/pays, si quelqu'un veut vous poursuivre pour infraction à la protection des droits d'auteur.
- Si un site ou un FAI distant interdit votre adresse IP à cause de quelque chose que vous faites, vous pouvez simplement passer à un autre serveur VPN ou à un autre service VPN.

Avantages (2/2)

- Flexibilité : vous pouvez activer et désactiver le VPN, ou changer de serveur VPN, comme vous le souhaitez.
- Ajoutez plusieurs juridictions/pays, si quelqu'un veut vous poursuivre pour infraction à la protection des droits d'auteur.
- Si un site ou un FAI distant interdit votre adresse IP à cause de quelque chose que vous faites, vous pouvez simplement passer à un autre serveur VPN ou à un autre service VPN.
- Si quelqu'un essaie de vous DDOS, le trafic va au serveur VPN, pas à votre adresse IP personnelle.

Avantages (2/2)

- Flexibilité : vous pouvez activer et désactiver le VPN, ou changer de serveur VPN, comme vous le souhaitez.
- Ajoutez plusieurs juridictions/pays, si quelqu'un veut vous poursuivre pour infraction à la protection des droits d'auteur.
- Si un site ou un FAI distant interdit votre adresse IP à cause de quelque chose que vous faites, vous pouvez simplement passer à un autre serveur VPN ou à un autre service VPN.
- Si quelqu'un essaie de vous DDOS, le trafic va au serveur VPN, pas à votre adresse IP personnelle.
- Certains VPN ont des fonctionnalités supplémentaires, telles que le blocage des publicités, le blocage des sites malveillants et le contrôle parental.

Inconvénients (1/2)

- Pénalité de performance probable

Inconvénients (1/2)

- Pénalité de performance probable
- Tarification

Inconvénients (1/2)

- Pénalité de performance probable
- Tarification
- Disfonctionnement de sites

Inconvénients (1/2)

- Pénalité de performance probable
- Tarification
- Disfonctionnement de sites
- Si vous installez l'application personnalisée du VPN sur votre système, vous faites confiance à l'application pour qu'elle ne soit pas malveillante.

Inconvénients (1/2)

- Pénalité de performance probable
- Tarification
- Disfonctionnement de sites
- Si vous installez l'application personnalisée du VPN sur votre système, vous faites confiance à l'application pour qu'elle ne soit pas malveillante.
- Le VPN peut interférer avec les opérations entre les appareils de votre réseau local, telles que les applications de transfert de fichiers ou de contrôle à distance ou d'égal à égal.

Inconvénients (1/2)

- Votre FAI doit obéir aux lois de votre pays ; le VPN peut être situé dans un pays étranger sous un système juridique différent. La société VPN peut être moins réglementée que votre FAI. Si le VPN partage des adresses IP entre de nombreux clients, vous pouvez souffrir du mauvais comportement des autres utilisateurs.

[<+->]

Inconvénients (1/2)

- Votre FAI doit obéir aux lois de votre pays ; le VPN peut être situé dans un pays étranger sous un système juridique différent. La société VPN peut être moins réglementée que votre FAI. Si le VPN partage des adresses IP entre de nombreux clients, vous pouvez souffrir du mauvais comportement des autres utilisateurs.
- Certains clients VPN peuvent planter/échouer en silence. Vous pouvez donc naviguer pendant un moment en pensant que vous utilisez le VPN, alors que vous ne l'êtes pas.

[<+->]

Une question de confiance

- Décryptage du trafic

Une question de confiance

- Décryptage du trafic
- Usurpation DNS

Une question de confiance

- Décryptage du trafic
- Usurpation DNS
- Usurpation HTTPS / Attaque d'homographe

Une question de confiance

- Décryptage du trafic
- Usurpation DNS
- Usurpation HTTPS / Attaque d'homographe
- SSL bumpingă: production de faux certificat TLS

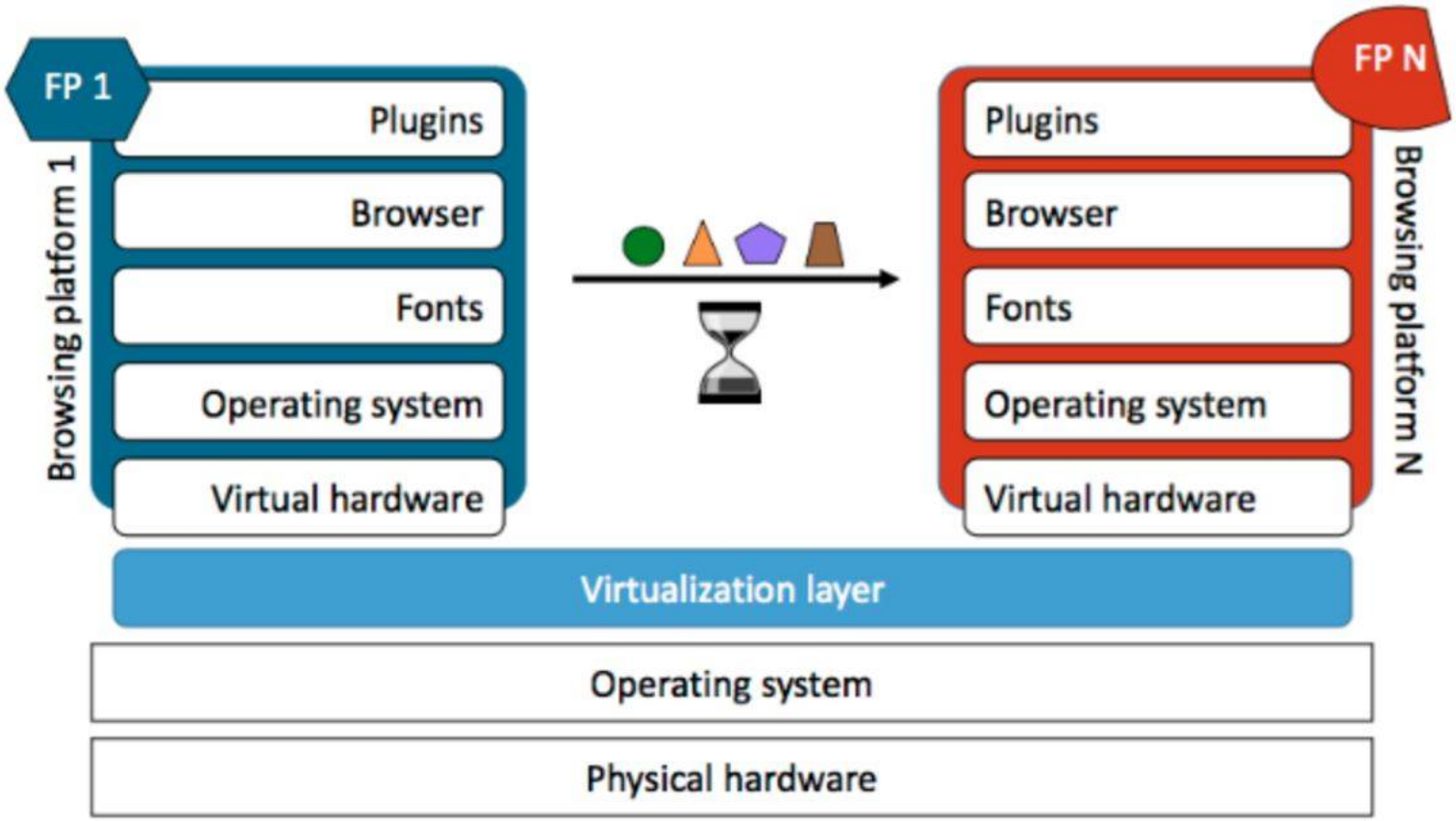
Une question de confiance

- Décryptage du trafic
- Usurpation DNS
- Usurpation HTTPS / Attaque d'homographe
- SSL bumpingă: production de faux certificat TLS
- Décapage SSLă: Réorientation du client Web

Une question de confiance

- Décryptage du trafic
- Usurpation DNS
- Usurpation HTTPS / Attaque d'homographe
- SSL bumpingă: production de faux certificat TLS
- Décapage SSLă: Réorientation du client Web
- Déclassement SSL / TLSă: seul TLS 1.0 est disponible !

Fingerprinting



AmIUnique

Webographie

- TODARO Cédric : Les RPV (Réseaux Privés Virtuels) ou VPN (VirtualPrivate Networks)
- Le VPN : `https://www.le-vpn.com`
- FormIp : `https://formip.com`
- Bill Dietrich : `https://www.billdietrich.me`