Votre fournisseur d'accès et vos données: choisir et paramétrer un VPN, choisir et configurer son serveur DNS

Pour naviguer sur internet, pour faire un lien entre votre ordinateur local et les pages d'un site Web, vous utiliser les routes du WEB et vous passer par un fournisseur d'accès ou FAI ou ISP. Les fournisseurs d'accès Internet sont généralement des entreprises, parfois des associations, françaises, qui ont obtenu une licence d'opérateur auprès de l'Autorité de Régulation des Communications Électroniques et des Postes (ARCEP www.arcep.fr) et qui peuvent faire une offre d'accès à leurs clients.
Dans le cas le plus général, les clients pourront, grâce à l'équipement fourni par le FAI et la ligne téléphonique, connecter leur propres ordinateurs ou mobile au réseau mondial en passant par la ligne que le FAI leur louent.

Toutes les données que le client d'un FAI recevra ou enverra sur le web mondial passera par le FAI, le FAI devra donc être un tiers de confiance pour vous.

Par ailleurs, l'état (pour nous l'état français), en votant des lois dites de sécurité intérieures (type LOPSI), imposera des règles de traçage et de stockage de vos communications, généralement directement ou facilement accessibles par les ministères de l'intérieur et de la justice en plus d'être exploitables par le FAI lui-même.

Vous pouvez avoir de bonnes raisons de vous protéger de ces regards et de vérifier l'usage qui sera fait de vos informations, aujourd'hui ou demain (une fois stockées, il est très difficile de maîtriser l'avenir d'une données dans le réseau mondial.

Nous parlons régulièrement dans nos ateliers de la notions de tiers de confiance, nous développerons à nouveau cette notion dans le cadre de cet atelier. Quel est le contrat qui me lie à mon fournisseurs d'accès, quels sont les contrats qui le lient avec des tiers, commercialise-t-il et avec qui les données qu'il stocke à mon sujet, filtre-t-il l'information qui m'arrivent en fonction d'algorithmes, etc

Si je ne veux pas accorder une confiance aveugle à l'entreprise ou l'association qui me fournit l'accès,

si je ne veux pas, systématiquement dire à qui je parle, stocker ce que je dis, lis ou regarde, à des tiers que je ne connais pas, il existe des façons de communiquer qui empêchent ou limitent les informations que je fais circuler d'être exploitées par mon FAI ou ses partenaires.

Nous en verrons deux, il en existe beaucoup d'autres. Mais avant cela, je peux prendre le temps de choisir mon tiers de confiance pour ce service, tous n'ont pas les mêmes qualités, les mêmes défauts, le même prix !

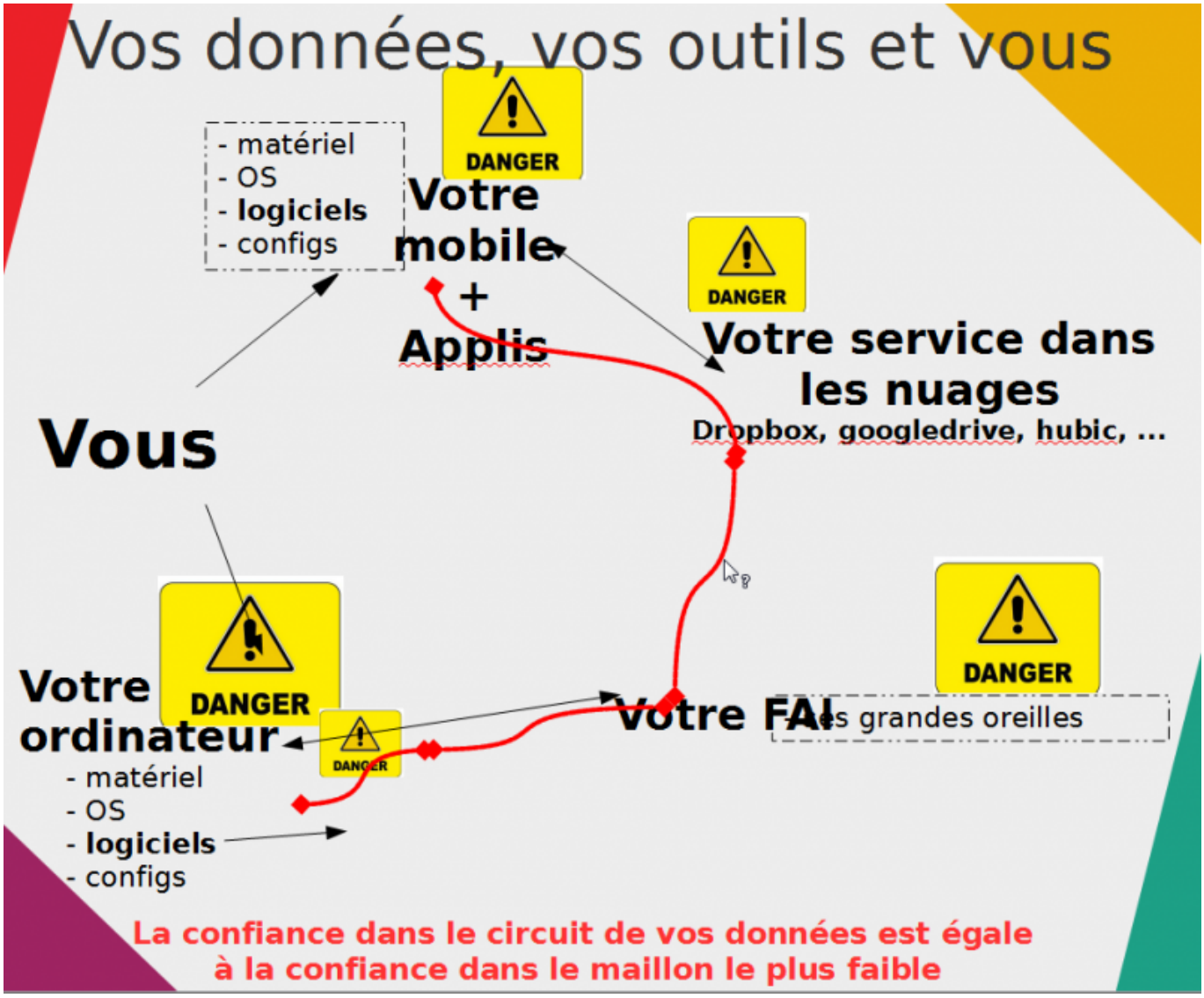
Quel FAI choisir ?

Les FAI auxquels il est possible de s'abonner en France n'est pas très importante et tend plutôt à diminuer. Toutefois, à côté des grands classiques qui proposent des offres groupées (Internet, Téléphonie, TV, Mobiles, ...), il existe d'autres fournisseurs plus spécialisés comme OVH plutôt orienté professionnels ou la FDN, associatifs militants qui proposent des services orientés vers la protection de la vie privée et la neutralité du Net. Au titre de cet atelier, la FDN est LE tiers de confiance “idéal”. |Article FAI sur Wikipédia

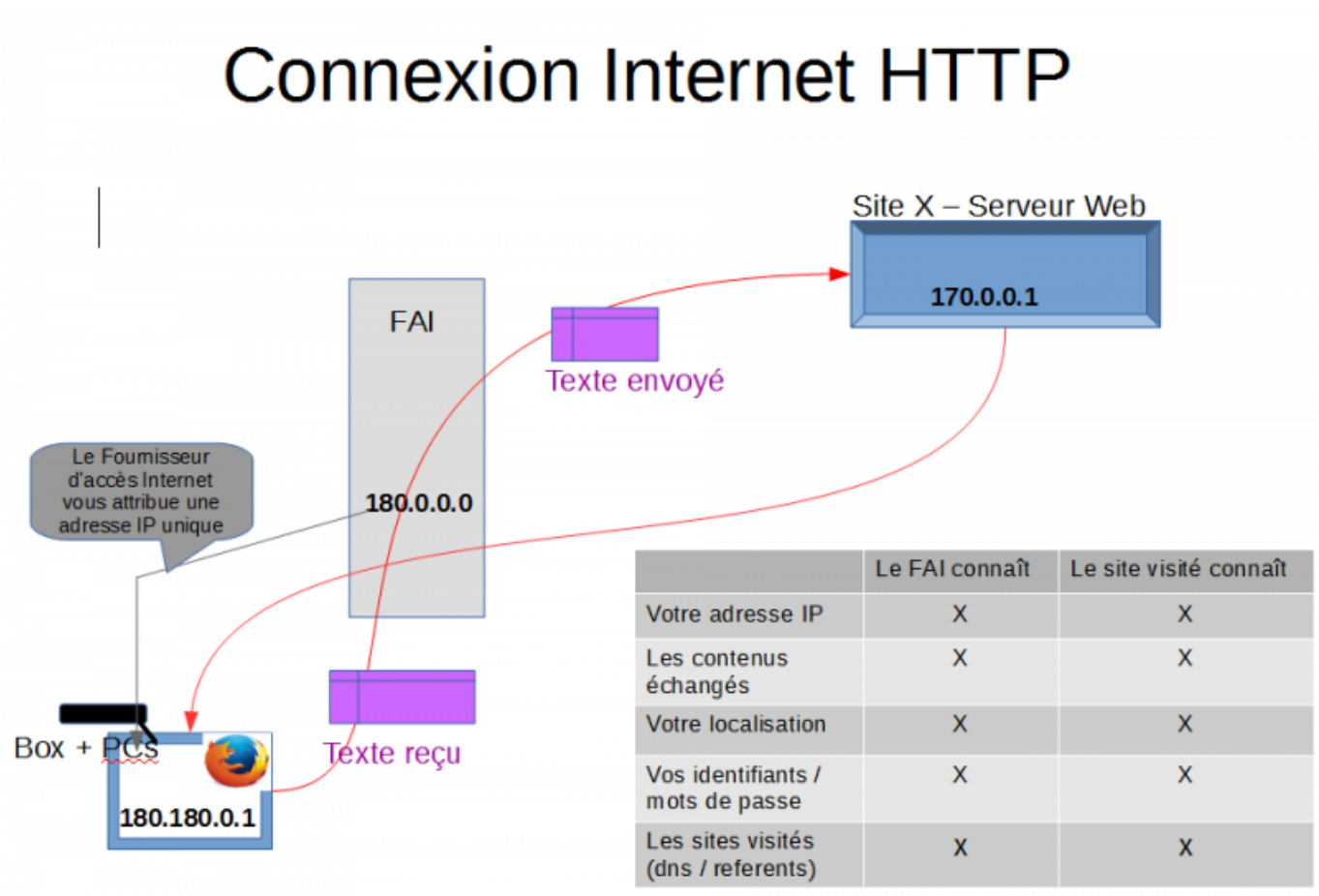
HTTP / HTTPS / VPN / TOR

Schémas de circulation des données

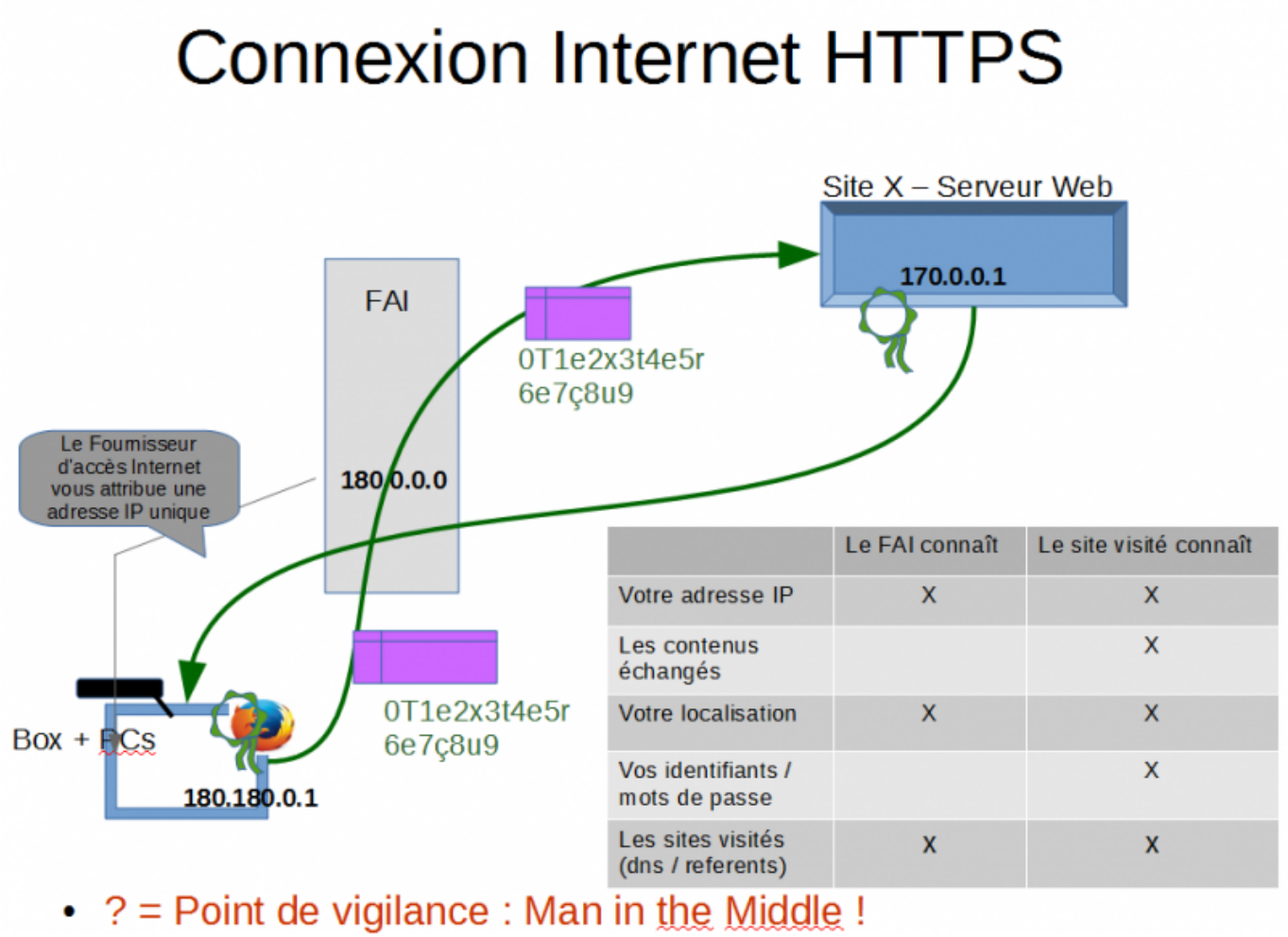
L'essentiel de notre atelier abordera les caractéristiques, avantages et risques liés à l'usage d'un VPN. Les données sur Internet sont vulnérables de plusieurs façons, lors de leur production (logiciels, OS mis en œuvre), sur leurs lieux de stockage (sur vos ordinateurs, chez votre FAI, sur les sites des tiers) et aussi pendant leur transport (ligne rouge dans le schéma ci-dessous).



Le visiteur derrière sa box se connecte à un site Les données circulent sur internet selon un protocole qui permet à des ordinateurs reliés en réseau de dialoguer.
Il existent de nombreux protocoles pour assurer ce transport, le plus connu et utilisé étant le HTTP.
Sous HTTP, voici une représentation du transport des données:

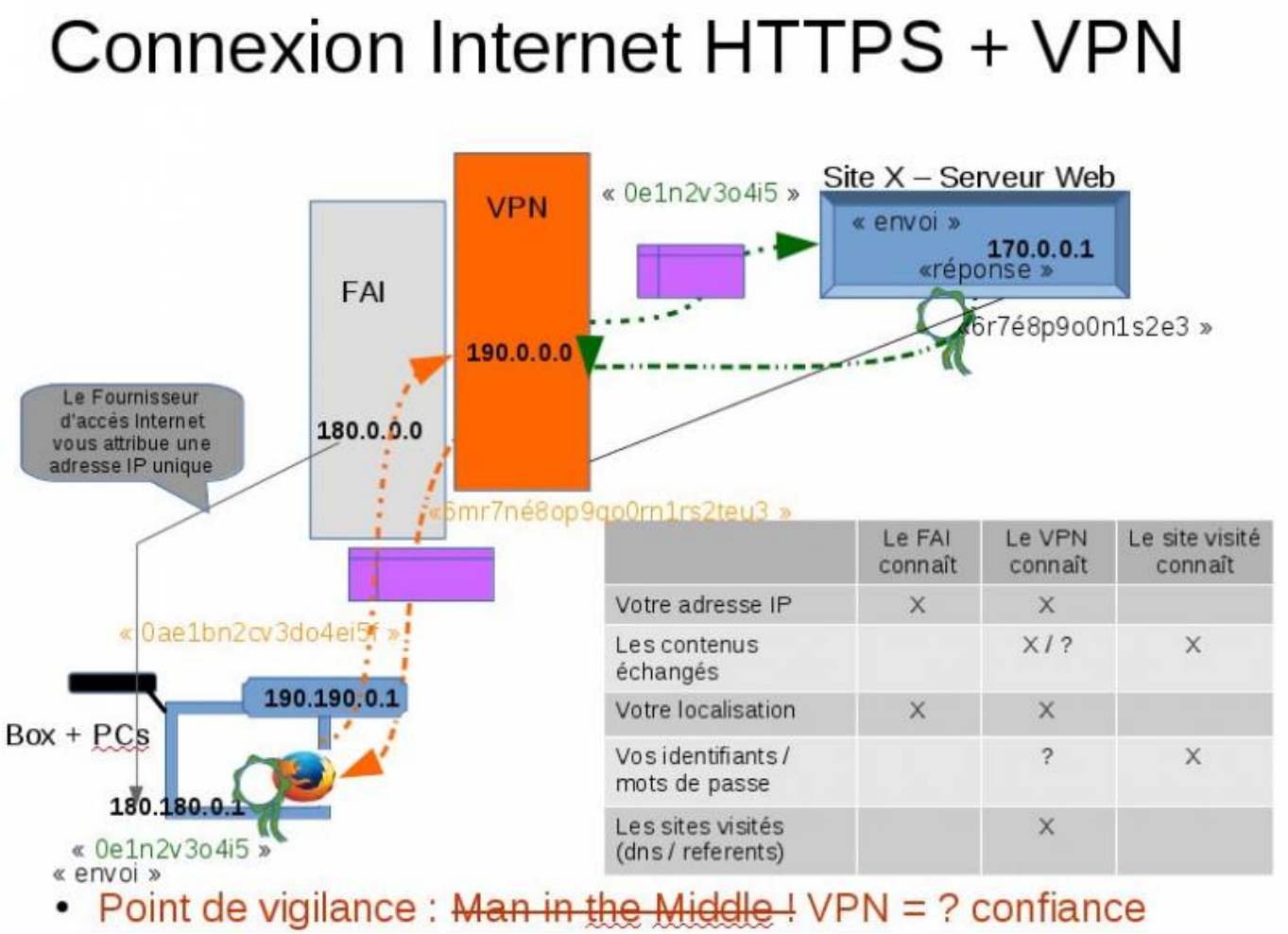


Les données transitent en clair (format texte classique, pas de chiffrement) tout le long du chemin de votre ordinateur au site visité et vice-versa (ici Texte reçu et Texte envoyé.
Données: Le FAI stocke toutes les données qui transitent pendant, à minima, une durée légale et peut leur appliquer toutes sortes d'algorithmes pour consolider votre profil. Les identifiants et mots de passe circulent en clair également.
Métadonnées: les adresses IP, dates et heures, destinataires et contacts, pages visitées et durées des visites, natures des matériels et logiciels utilisés sont stockées par le FAI et les pages visitées des sites consultés.



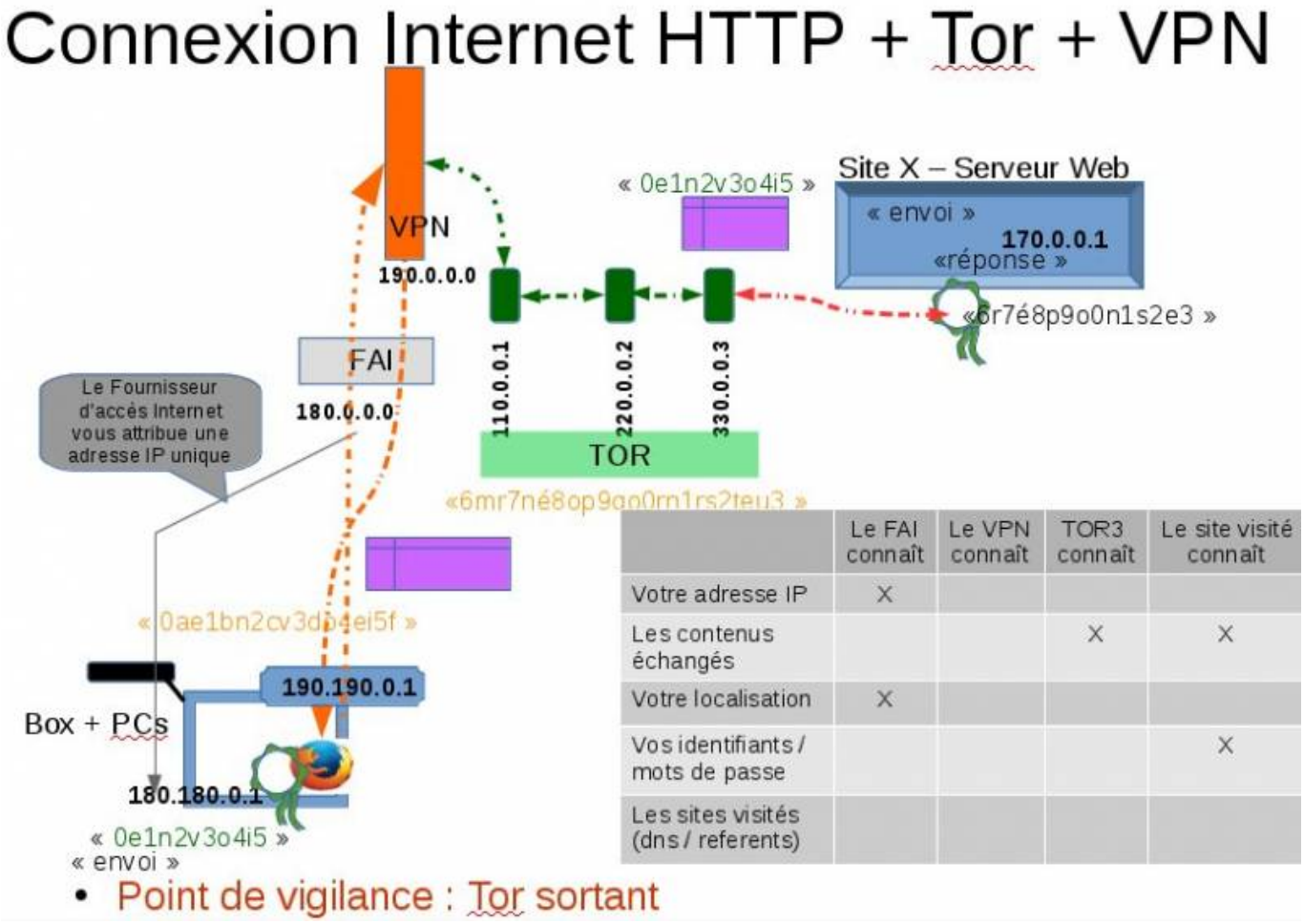
	Le FAI connaît	Le site visité connaît
Votre adresse IP	X	X
Les contenus échangés		X
Votre localisation	X	X
Vos identifiants / mots de passe		X
Les sites visités (dns / referents)	X	X

Les données sont chiffrées par le navigateur avec la clé certifiée échangée avec le serveur destinataire et lisibles seulement par lui, elles transitent en format codé tout le long du chemin de votre ordinateur au site visité et vice-versa (ici 0T1e2x3t4e5r6e7ç8u9).
Données: Le FAI stocke toutes les données qui transitent pendant, à minima, une durée légale mais ne sont pas lisibles par lui, il ne peut donc pas leur appliquer d'algorithmes pour consolider votre profil. Les identifiants et mots de passe circulent en format chiffré.
Métadonnées: les adresses IP, dates et heures, destinataires et contacts, pages visitées et durées des visites, natures des matériels et logiciels utilisés sont stockées par le FAI et les pages visitées des sites consultés.



Les données sont d'abord chiffrées par le navigateur avec la clé échangée avec le serveur destinataire, puis chiffrées une deuxième fois par la connexion réseau avec la clé certifiée du serveur VPN, elles transitent par le FAI en format chiffré 2 fois depuis votre ordinateur jusqu'au serveur VPN qui déchiffre le chiffrement VPN et envoie le contenu chiffré une fois par la clé certifiée HTTPS vers le destinataire qui est alors capable de déchiffrer le primo chiffrement et lire le contenu. La réponse se fait par le chemin inverse selon les mêmes modalités (ici 6mr7né8op9qo0rn1rs2teu3).

Données: Le FAI stocke toutes vos données qui transitent; elles sont chiffrées deux fois avec deux clés différentes mais ne sont pas lisibles par lui, il ne peut donc pas leur appliquer d'algorithmes pour consolider votre profil.
Il ne connait que le destinataire VPN (il ne sait donc pas quel site vous visitez, ni votre adresse IP d'origine.
Le serveur VPN sait par contre quel site vous visitez et votre adresse IP d'origine, il ne connait pas le contenu de vos données sauf si vous visitez un site non chiffré (en HTTP).
La protection est totale vis à vis du FAI, partielle vis à vis du serveur VPN, en bref, **vous déplacez votre tiers de confiance du FAI au serveur VPN**.
Les identifiants et mots de passe circulent en format doublement chiffré.
Métadonnées: les adresses IP, dates et heures, destinataires et contacts, pages visitées et durées des visites, natures des matériels et logiciels utilisés sont stockées par le FAI mais inutilisables par lui et les pages visitées des sites consultés.

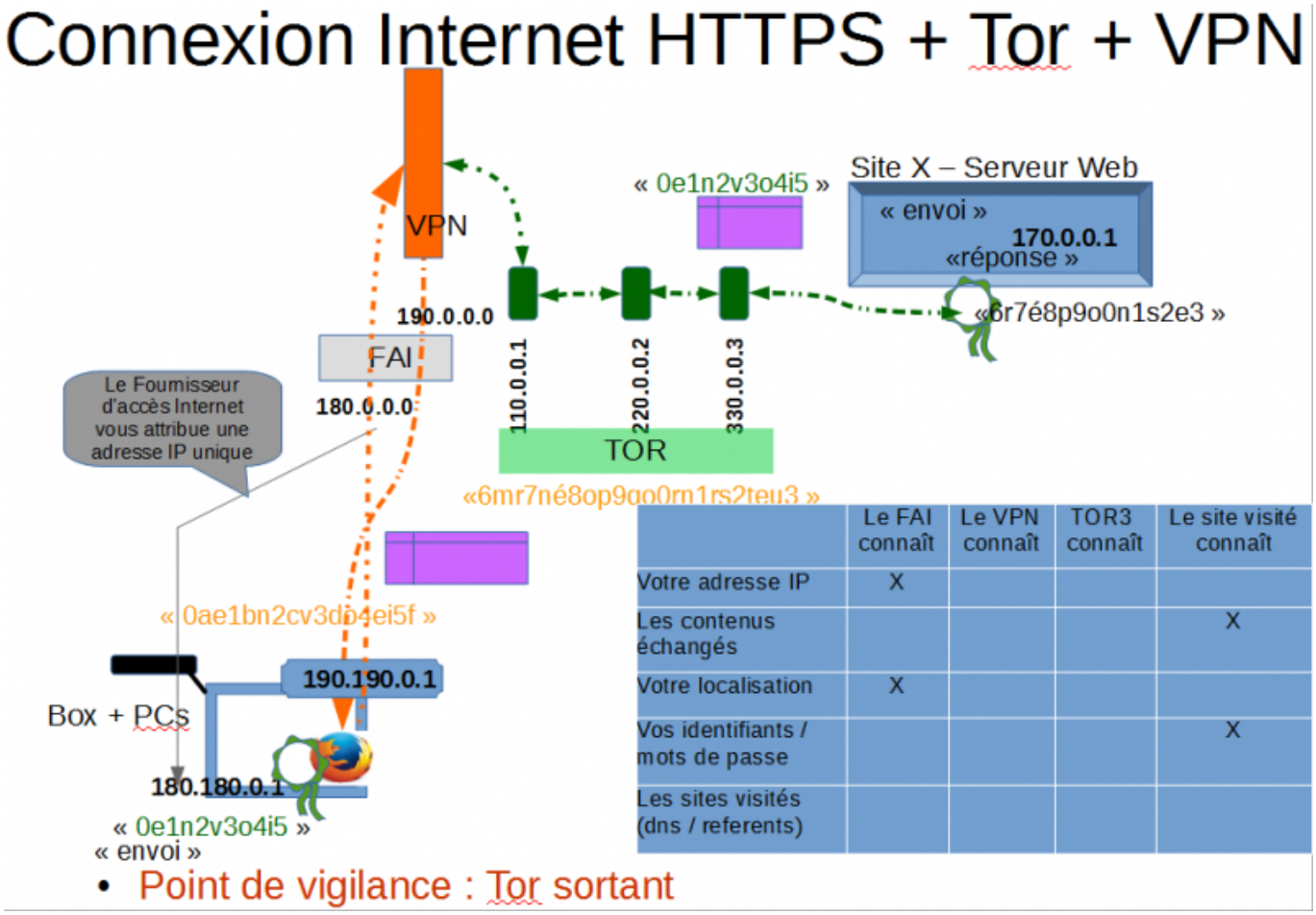


	Le FAI connaît	Le VPN connaît	TOR3 connaît	Le site visité connaît
Votre adresse IP	X			
Les contenus échangés			X	X
Votre localisation	X			
Vos identifiants / mots de passe				X
Les sites visités (dns / referents)				

Les données sont d'abord chiffrées par le navigateur TorBrowser avec les clés certifiées des serveurs TOR, puis chiffrées une quatrième fois par la connexion réseau avec la clé certifiée du serveur VPN, elles transitent par le FAI en format chiffré 4 fois depuis votre ordinateur jusqu'au serveur VPN qui déchiffre la sécurité VPN et envoie le contenu encore chiffré trois fois par les clés des serveurs TOR vers un premier serveur TOR (garde), puis un second serveur TOR en enfin un 3ème serveur TOR (sortant) qui envoie alors le contenu déchiffré au site visité.
Le site peut vous envoyer une réponse qui se fait par le chemin inverse selon les mêmes modalités (ici 6mr7né8op9qo0rn1rs2teu3).

Données: Le FAI stocke toutes vos données qui transitent; elles sont chiffrées 4 fois avec 4 clés différentes mais elles ne sont pas lisibles par lui, il ne peut donc pas leur appliquer d'algorithmes pour consolider votre profil.
Il ne connaît que le destinataire VPN (il ne sait donc pas quel site vous visitez, ni votre adresse IP d'origine.
Le serveur VPN ne sait pas quel site vous visitez ni votre adresse IP d'origine, Il ne connaît pas le contenu de vos données.
La protection est totale vis à vis du FAI et du serveur VPN mais pas à la sortie TOR, Le serveur VPN envoie vos données chiffrées en oignon à trois serveurs TOR successifs, dernier, nommé sortant, envoie le paquet original non chiffré au serveur visité.
Ici, **vous déplacez votre tiers de confiance du VPN au serveur TOR sortant**.
Les identifiants et mots de passe circulent jusqu'au serveur TOR sortant en format plusieurs fois chiffré.
Pour rendre le traçage des utilisateurs de TOR encoure plus complexes, le système TOR change le chemin de de transit de vos données toutes les n minutes, le serveur sortant ne transite pas forcement toutes les données d'un même échange.

Métadonnées: les adresses IP, dates et heures, destinataires et contacts, pages visitées et durées des visites, natures des matériels et logiciels utilisés et les pages visitées des sites consultés sont stockées par le FAI mais inutilisables par lui.



	Le FAI connaît	Le VPN connaît	TOR3 connaît	Le site visité connaît
Votre adresse IP	X			
Les contenus échangés				X
Votre localisation	X			
Vos identifiants / mots de passe				X
Les sites visités (dns / referents)				

Les données sont chiffrées par le navigateur avec la clé certifiée échangée avec le serveur destinataire et lisibles seulement par lui, elles sont ensuite chiffrées par le même navigateur TorBrowser avec les clés certifiées des serveurs TOR, puis chiffrées une cinquième fois par la connexion réseau avec la clé certifiée du serveur VPN.
Elles passent donc chiffrées 5 fois chez le FAI, puis transitent par le serveur VPN où elles seront déchiffrées (on passe de 5 couches à 4 couches), transitent par les 3 serveurs TOR qui déchiffrent tour à tour leur chiffrement et ressortent du troisième serveur TOR avec 1 niveau de chiffrement par la clé certifiée HTTPS visité (destinataire).
Le chemin retour se fera de la même façon, dans l'autre sens.

Données: Le FAI stocke toutes vos données qui transitent; elles sont chiffrées 5 fois avec 5 clés différentes, elles ne sont donc pas lisibles par lui, il ne peut donc pas leur appliquer d'algorithmes pour consolider votre profil.
Il ne connaît que le destinataire VPN (il ne sait donc pas quel site vous visitez, ni votre adresse IP d'origine.
Le serveur VPN ne sait pas quel site vous visitez ni votre adresse IP d'origine, Il ne connaît pas le contenu de vos données.
La protection est totale vis à vis du FAI et du serveur VPN, Le serveur VPN envoie vos données chiffrées en oignon à trois serveurs TOR successifs. Le dernier, nommé sortant, envoie vers le serveur

visité le paquet chiffré avec la clé certifiée échangée avec lui.
Ici, la confiance peut être estimée comme maximale, seul le site visité connaît vos données mais les métadonnées qui lui sont fournies sont réduites au minimum.
Les identifiants et mots de passe circulent jusqu'au serveur TOR sortant en plusieurs fois chiffré.
Pour rendre le traçage des utilisateurs de TOR encoure plus complexes, le système TOR change le chemin de de transit de vos données toutes les n minutes, le serveur sortant ne transite pas forcement toutes les données d'un même échange.
Métadonnées: les adresses IP, dates et heures, destinataires et contacts, pages visitées et durées des visites, natures des matériels et logiciels utilisés sont stockées par le FAI mais inutilisables par lui et les pages visitées des sites consultés.

Choisir et utiliser un VPN

Comme nous pouvons le constater dans les schémas précédents, le fournisseur de serveur VPN doit pouvoir être un tiers de confiance au moins aussi voir plus fiable que le fournisseur d'accès.
Quels critères utiliser pour juger de la confiance qu'on peut accorder à un fournisseur VPN ?
Les critères qui valent pour choisir un fournisseur VPN sont grosso-modo les critères qui valent pour tous les services internet. En voici quelques par ordre de priorités:

1. **dans quel pays exerce-t-il sont activité ?**
   La législation qui s'applique à votre contrat est la législation du pays du fournisseur de service. La législation du pays du client peut être amenée à faire appel à la juridiction du pays du fournisseur.
   quelles sont les droits en cours dans le pays du fournisseur, quelle est la jurisprudence dans ce même pays, quelles y sont les tendances législatives, quelles sont les relations juridiques entre le pays du client et le pays du fournisseurs ?
   Toutes ces questions peuvent trouver réponse, à condition de prendre du temps. Mes les lois des pays et les relations entre les pays évoluent, parfois vite.
   Alors pourquoi se donner tant de mal, de plus sans possibilité d'exercer son pouvoir citoyen dans le dit pays ?
   Il semble que tout porte à conseiller de souscrire à des services dans le pays où on habite, surtout pour des activités légales.
   Une fois le pays choisi, on peut passer au choix du fournisseur dans le pays; à côté des fournisseurs uniquement marchands et donc soumis à leurs impératifs commerciaux pas, on peut (on doit ?) rechercher un fournisseur qui milite pour la protection de la vie privée sur internet, pas seulement avec des mots mais aussi avec des engagements clairs, explicites et non équivoques.
2. **quel est son modèle économique ?**
   se méfier des services gratuits (la mise en œuvre de plateformes VPN coûte chère, en investissement, en fonctionnement, en performance … pour autant, payant ne veut pas dire vertueux !
3. quelle licence vous impose-t-il de signer ?
   lire la licence d'un service, gratuit ou payant, sur internet est incontournable même si cela est fastidieux; vous pourrait toujours vous faire aider pour cette lecture. Des personnes compétentes pourront aider, à la médiathèque également.
4. **quelle charte d'utilisation vous propose-t-il ?**
   voir licence
5. **quelle est sa réputation, sa e-réputation** ?
   comme pour la plupart des services internet, il existe des comparatifs, des remarques

d'utilisateurs, des actualités de plaintes et des controverses avec des clients ou des anciens clients ...

Des conseils:
La FFDN “fédération qui regroupe des Fournisseurs d'Accès à Internet associatifs se reconnaissant dans des valeurs communes : bénévolat, solidarité, fonctionnement démocratique et à but non lucratif; défense et promotion de la neutralité du Net.” dont fait partie la FDN ou des CHATONS comme Zaclys proposent des services de qualité pour particuliers.
Orbot et Bitmask sont d'excellente solutions VPN pour Android sur vos Ttablettes et Smartphones

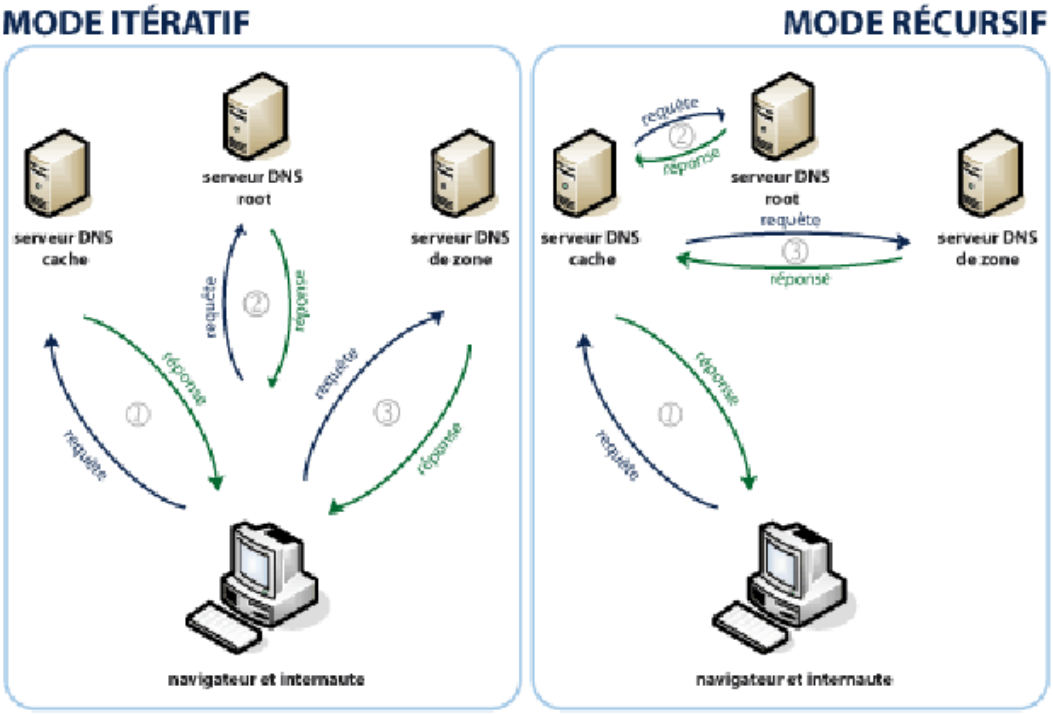
Choisir et utiliser un service DNS (Serveur DNS = serveur de noms)

DNS: The whole internet runs on it!

Les DNS sont nés en 1983 du besoin de remplacer une adresse IP par une forme d'identification de l'adresse cible plus facile à retenir.
Depuis, ils sont partout: dans les entreprise, chez les hébergeur, chez les fournisseur d'accès Internet, chez les fournisseurs de noms de domaine (registrar).

Les serveurs DNS permettre de faire une *résolution* d'adresses textes en adresses IP,

Le mécanisme en œuvre quand vous accédez à un site Internet est le suivant: votre requête est envoyée au serveur DNS de rattachement (celui de votre entreprise ou de votre FAI) qui répond s'il connaît la réponse ou interroge les serveurs DNS (dit racines) sinon ... jusqu'à ce qu'il trouve la réponse qu'il renvoie alors au navigateur de votre ordinateur. Cela peut fonctionner selon deux modes: un mode itératif ou un mode récursif



L'adressage au serveur DNS passe généralement par un serveur primaire qui contient le source des informations et d'un serveur secondaire synchronisé avec le serveur primaire. Le but est d'obtenir une disponibilité maximale. Le DNS de rattachement peut mettre en cache les informations qu'il obtient suite à une demande par les navigateurs.
Lorsque vous utilisez les serveurs DNS de votre fournisseur d'accès, celui-ci peut connaître, stockez, historiser toutes adresses des sites que vous visitez et, par des algorithmes, en tirer des informations précises sur votre profil. Il peut aussi censurer certains sites en les rendant impossible ou difficile à atteindre.
La FDN, tiers de confiance déjà cité, propose des résolveurs DNS récursifs ouverts, vous les trouverez sur leur site à l'adresse https://www.fdn.fr/actions/dns/

Connaître le serveur DNS que j'utilise ?
Nameserver Resolver Diagnostic Tool
What's my IP, DNS Resolver, EDNS Client Subnet and Geolocalization?

Allez plus loin ...

Page Wikipedia Réseau privé virtuel
Page Wikipedia DNS
Comment le VPN Riseup fonctionne
VPN, les autres intérêts que la sécurité
Serveurs DNS des principaux FAI
Fonctionnement DNS merci pour les illustrations
Un MOOC pour tout savoir sur le DNS

— *André Vanderlynden* *2018/10/03 22:00*