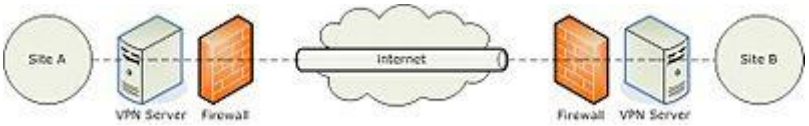
Réseau privé virtuel (VPN).

(extrait de formation en cybersécurité)



Principe d'un VPN simple

En informatique, un **réseau privé virtuel**, plus communément abrégé en **VPN** (de l'anglais : *virtual private network*), est un système permettant de créer un lien direct entre des ordinateurs distants, qui isole leurs échanges du reste du trafic se déroulant sur des réseaux de télécommunication publics.

La connexion entre les ordinateurs est gérée de façon transparente par un logiciel de VPN, créant un tunnel entre eux. Les ordinateurs connectés au VPN sont ainsi sur le même réseau local (virtuel), ce qui permet de passer outre d'éventuelles restrictions sur le réseau (comme des pare-feux ou des proxys).

Le VPN peut être avec ou sans client spécifique.

Les principales utilisations VPN pour les postes clients

Le VPN SSL (Sans utilisation d'un logiciel spécifique.)

Aussi appelé « *clientless* », car il ne nécessite pas l'installation d'un logiciel client ; un navigateur Web compatible avec l'ouverture des sessions HTTPS SSL/TLS est suffisant.

Le VPN IPsec (Le plus connu)

L'installation d'un logiciel « agent » est nécessaire afin d'établir un tunnel vers un serveur VPN.
Les adresse IP sont changées. (Vous pouvez télécharger un film sur votre ordinateur en France depuis une adresse IP de Pologne).

Exemple : Vous Utilisez NordVPN (ou Mozilla VPN).

Quand vous lancer NordVPN sur votre ordinateur avec comme serveur la Pologne vous créez un VPN entre votre ordinateur et un serveur de NordVPN en Pologne et c'est ce serveur qui fera vos « request » Internet à votre place. Donc, les sites que vous solliciterez penseront que vos demandes viennent de Pologne et non de France.
Cela vous met à l'abri des surveillances faites par ADOPI ou autres, pour interdire le téléchargement de fims. (Indispensable si vous utilisez des « Torrent ».)

Deux Types d’utilisations.

Utilisation point à point sécurisé.

Un VPN permet d'accéder à des ordinateurs distants comme si l'on était connecté au réseau local. Il permet d'avoir un accès sécurisé au réseau interne d'entreprise, ou de créer un réseau de pairs. Par exemple c’est l’utilisation type sécurisé pour le télétravail.

Utilisation comme passerelle.

Un VPN dispose généralement aussi d'une « passerelle » permettant d'accéder à l'extérieur, ce qui permet de changer l'adresse IP source apparente de ses connexions. Cela rend plus difficile l'identification et la localisation approximative de l'ordinateur émetteur par le fournisseur de service. C’est l’outil parfait pour télécharger des contenus interdit. (Vidéo, Films, logiciels etc..)

L'utilisation de VPN n'est généralement pas légalement restreinte.

Elle l'est en Chine . Surtout depuis Septembre 2017, il semble que la Chine ait décidé de resserrer l'accès des Chinois à Internet en accroissant la répression pour ceux qui utilisent des réseaux privés virtuels (VPN) (et donc non-contrôlés par le gouvernement).

Chiffrement

Les connexions VPN ne sont pas nécessairement chiffrées. Cependant si l'on ne chiffre pas, cela peut permettre à des éléments intermédiaires sur le réseau d'accéder au trafic du VPN, ce qui peut être problématique si les informations qui y transitent sont sensibles.

Les VPN payants sont chiffrés.

VPN dans les environnements mobiles

Les VPN mobiles sont largement utilisés dans la sécurité publique où, par exemple, ils donnent aux agents des forces de l'ordre l'accès à des applications telles que les bases de données criminelles. C’est la sécurité point à point des VPN qui est utilisé dans ce cas-là.

Inconvénients des VPN.

Quand on utilise un VPN en tant que passerelle que ce soit sur un poste fixe ou sur son smartphone, on fait paraitre une adresse IP qui n’est pas la sienne. Beaucoup de logiciels utilisent maintenant l’adresse IP comme deuxième référence pour sécuriser une identification. Il est probable que si vous utilisez un VPN, vous ne puissiez plus accéder à votre banque ou a NETFIX.