OpenVPN : Roadwarrior

Samuel Monier 3 février 2015

Vous avez suivi les deux premiers articles sur OpenVPN. Vous avez donc appris à mettre en place un tunnel VPN très simplement, pour des besoins de tests ici, puis vous avez poursuivi avec la mise en place d'une vraie solution sécurisée sur infrastructure PKI ici. Maintenant que vous avez découvert le potentiel d'OpenVPN, je vais vous présenter une configuration spécifique aux clients itinérants.

Afin de mettre en place cette configuration, il est nécessaire de passer par les deux articles précédents sur OpenVPN.

Article 1 : OpenVPN point-to-point

Article 2 : OpenVPN PKI

Roadwarrior

Tout d'abord, qu'est ce que signifie « roadwarrior »? Non, rien à voir avec le titre en VO du deuxième épisode de Mad Max! Dans le domaine des réseaux informatiques, une configuration de type « roadwarrior » signifie plusieurs choses :

- Un client mobile, constamment en mouvement
- Un client qui a besoin d'un accès internet
- Un client qui a besoin d'accéder aux ressources d'entreprise

C'est ce dernier point qui fait qu'on entend le mot « roadwarrior » presque exclusivement quand on parle de VPN. Le meilleur moyen pour un client nomade d'accéder aux données de l'entreprise, voir aux logiciels et autres ressources, c'est d'utiliser un VPN.

Ces notions sous-entendent, en terme de configuration réseau :

- Que l'accès se fera par divers moyens (hotspot, wifi d'hôtel, wifi d'un

client visité, téléphone mobile en mode modem)
- Qu'on ne maitrise pas du tout la configuration de ces points d'accès
- Qu'on a besoin de confidentialité, puisqu'on ne maitrise pas la sécurité du réseau

Mettre en place une configuration « roadwarrior », au final, c'est adapter notre VPN à ces problématiques.

Utilisation de ports biens connus

Pour répondre au manque de maitrise du réseau, nous allons devoir adapter notre configuration.
En effet, nous devons supposer que le réseau qu'utilisera par exemple notre technico-commercial en itinérance, sera mis en place par un bon tech, un peu parano sur la sécurité, et que par défaut, il veillera à ce que **tous les ports du firewall soient bloqués**. Il estimera par exemple, dans le cas d'un hôtel, qu'on laisse uniquement l'accès à internet pour les clients.

Notre commercial lancera donc son client OpenVPN, et là, le tunnel ne montera pas. Hé oui!! Le port 1194, utilisé par défaut sur OpenVPN est bloqué.

L'astuce consiste donc à modifier la configuration de notre VPN afin de lui faire utiliser des ports qui sont libres partout, à priori. Nous allons choisir des ports qui sont nécessaires aux connexions web simples :

- **Port 443** (HTTP sur TLS/SSL)
- **Port 80** (HTTP)
- **Port 53** (DNS)

Ces ports sont forcément ouverts, ils constituent donc un bon choix. Pour ma part, j'utilise le port **443**, c'est donc ce que nous allons voir dans la configuration.

TCP vs UDP

Reste un dernier choix : **TCP** ou **UDP**?

Je ne vais pas vous faire un cours magistral sur TCP et UDP. Je vais simplement tenter de vous expliquer rapidement les différences radicales entre ces deux protocoles.

La première différence est qu'un protocole est « orienté connexion » (TCP) par rapport l'autre qui est « orienté non-connexion » (UDP). En gros, UDP n'inclue aucun contrôle de la communication. Le flux de données est transmis, sans se soucier de la bonne réception. On a tendance à l'assimiler aux communications en LAN pour cette raison. TCP, lui, intègre des accusés de réception et contrôle CRC. C'est à dire qu'une machine sait si l'intégralité (et l'intégrité) des données envoyées sont reçues. Si un soucis arrive, les données peuvent être renvoyées.

Par défaut, OpenVPN fonctionne sur le port 1194, et sur le protocole **UDP**. Ce protocole de communication permet en effet une vitesse de transmission un peu plus élevée, du fait des fonctions de contrôles qui ne sont pas inclues. Cependant, si votre connexion internet n'est pas irréprochable (côté serveur ou client), ceci peut entraîner une plus grande répétition de paquets. Et de ce fait, la vitesse réelle de communication est bien en dessous.

Bon, alors on change systématiquement la configuration pour utiliser TCP? Oui, OpenVPN sait fonctionner avec TCP, il suffit de lui préciser. Cependant, il existe des avantages et des inconvénients. Voyons d'abord les inconvénients. TCP consacre une partie de sa « capacité » (en résumant très simplement) à inclure des données qui servent à assurer les fonctions de contrôles. Du coup, si la connexion est de bonne qualité, TCP sera moins performant, car moins de données sont transmises dans chaque paquet! Et le deuxième point négatif, c'est qu'il n'est pas conseillé d'encapsuler TCP dans TCP. Les paquets sont parfois mal interprétés, et ça demande plus de ressources de calcul au client et au serveur.

TCP	UDP
Reliable	Unreliable
Connection-oriented	Connectionless
Segment retransmission and flow control through windowing	No windowing or retransmission
Segment sequencing	No sequencing
Acknowledge segments	No acknowledgement

Bon, alors qu'est ce qu'on fait?

Dans notre cas, pour une connexion de type « Roadwarrior », le but est de mettre en place une connexion qui puisse être utilisable à coup sur depuis n'importe quel point d'accès. Et le protocole HTTPS, sur le port 443, lui, utilise TCP. Donc **TCP**!!
C'est pratiquement indétectable pour un firewall classique (il faut par exemple utiliser du stateful inspection pour détecter que le flux est suspect), c'est donc exactement ce qu'il nous faut!!

Configuration

C'est terriblement simple... Éditez vos fichiers de configuration (vous commencez à savoir faire!) et apportez ces modification :

Serveur

Remplacez **port 1194** par **port 443**

Décommenttez la ligne **proto tcp** et commentez la ligne **proto udp**

Client

Décommenttez la ligne **proto tcp** et commentez la ligne **proto udp**

Après le nom ou l'adresse IP du serveur distant, remplacez le port **1194** par **443**

Pas vraiment complexe!

Il ne vous reste qu'une chose à faire : Sur votre firewall, redirigez les connexions entrantes sur le port 443 vers l'adresse IP du serveur. Maintenant, c'est bon, vous pourrez accéder à votre serveur VPN de n'importe où!!

Astuce

Même si je ne devrais pas forcément le préciser, imaginez bien toute la portée d'un telle configuration : Pour une entreprise, elle permet par exemple à un commercial d'accéder aux ressources de l'entreprise depuis n'importe quelle chambre d'hôtel! Mais pour un particulier, monter un petit serveur VPN chez soit (avec un Rapsberry par exemple), permet de contourner toutes les restrictions d'un firewall depuis son lieux de travail! EN clair, on créer un tunnel entre son pc et son serveur, puis on fait ce qu'on veut. Sachez quand même deux choses : Du coup, vous sortez sur internet depuis chez vous, donc avec votre adresse IP. Et ensuite, il existe quand même des moyens de repérer un VPN encapsulé sur 443/TCP, même si c'est un peu complexe...

Puisque vous êtes encore là...

...Si cet article vous a aidé ou informé, laissez-moi vous demander une petite faveur. Nombreux d'entre vous utilise AdBlock sur **tech2tech**. Alors n'hésitez pas à désactiver AdBlock sur ce site ou bien à faire un don pour m'aider à couvrir les frais autour du site.

Si chacun de ceux qui ont lu et apprécié cet article participe, le futur de

tech2tech ne pourra être que meilleur. **Merci à vous !**.

FAIRE UN DON