Situation professionnelle en PPE 3 : Filtrage des accès internet vers internet via un PROXY

Documentation n°6 : Mise en place d'un accès VPN distant.

Auteur : Guillaume Orlando

Date : 11/12/2017

I. Création des certificats requis.

La méthode d'authentification retenu pour l'accès au serveur VPN distant se fera sur la présence d'un certificat VPN sur la machine cliente et un couple d'identifiant + mot de passe correspondant au compte d'un utilisateur VPN défini au sein du Pfsense.

Il nous faut donc générer ces certificats. Nous partons du principe que les documentations précédentes ont été appliqués à la lettre, et que la machine Pfsense est déjà une autorité de certification possédant le FQDN suivant : pfSense.btsio.lan

Nous aurons besoin de deux certificats : un certificat utilisateur et un certificat serveur.

Le premier sera à ajouter manuellement en tant que certificat interne. Le détail de la génération du certificat ne sera pas détaillé ici même, puisque nous avons maintenant plusieurs certificats à notre actif. Il faudra simplement faire attention à renseigner notre autorité de certification, à ajouter le FQDN du serveur Pfsense en Common Name ainsi qu'à spécifier que le certificat est un certificat de type utilisateur :

Nous pouvons faire de même en modifiant uniquement le type de certificat : ce sera ici un certificat serveur :

Maintenant que nos deux certificats sont faits, nous pouvons commencer à paramétrer le serveur OpenVPN.

II. Création du serveur OpenVPN.

La création du serveur VPN va être relativement simple, puisque Pfsense dispose d'un guide pas-à-pas pour la création de serveur OpenVPN. Pour le lancer, rendez-vous sous "'VPN" > "OpenVPN" puis sous "Wizards" :

Nous allons devoir renseigner un certain nombre d'informations diverse avant de créer le serveur en lui même. Dans un premier temps, nous spécifions que l'authentification se fait via un compte utilisateur local :

Nous indiquons ensuite notre autorité de certification interne :

Puis le certificat serveur créé précédemment :

Les paramètre du serveur VPN s'ouvrent ensuite à nous. Nous indiquons que le serveur VPN sera effectif sur l'interface WAN du notre Pfsense, en utilisant le protocole UDP et le port par défaut 1194, de façon à correspondre aux règles de pare-feu ajoutée dans les documentations précédentes :

Il faudra aussi spécifier une plage d'adresses relative aux IP délivrées au sein du tunnel VPN, ainsi qu'indiquer la possibilitée de contacter les machines présentes sur notre LAN depuis le tunnel VPN :

Enfin, si nos règles de pare-feu ne sont pas bonnes, ou si elles n'ont pas été faites au préalable, il nous reste la possibilitée de les ajouter automatiquement :

Et voilà, notre Serveur OpenVPN devrait maintenant être disponible dans la rubrique "VPN" > OpenVPN" > "Servers".

III. Création de l'utilisateur VPN.

Terminons par ajouter l'utilisateur VPN. L'ajout de celui-ci se fait sous "System" > "User Manager".

L'identifiant et le mot de passe de cet utilisateur seront ceux de connexion du VPN.

Attention à bien lier le certificat utilisateur à cet utilisateur :

Nous allons maintenant pouvoir exporter le package OpenVPN de cet utilisateur, dans un format compilé au sein d'un exécutable prêt à installer le client OpenVPN et les informations d'identifications requises.
Pour initier la connection à distance, il suffira de lancer le gestionnaire de connexions OpenVPN, puis de cliquer sur "connection".
Un message Windows nous informera si la connexion VPN fonctionne comme il faut.

Il sera alors possible d'accéder aux ressources réseaux du LAN, et notamment à la page d'administration du Pfsense, à distance.