Rapport SAE 401 : Sécurisation d’un SI

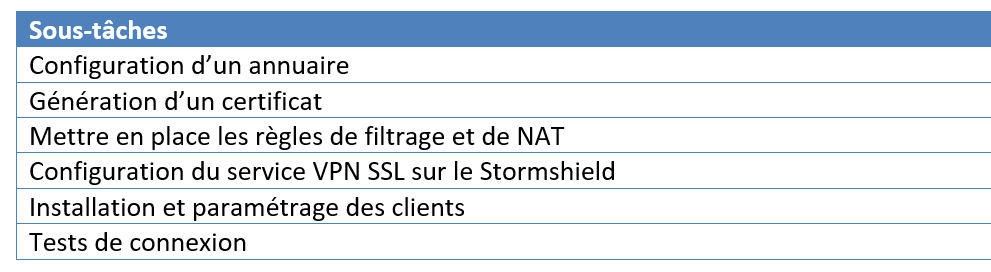
Participant : AZIZ Souhayl

Tâche 12 : Configuration d’un VPN SSL pour clients distants

Pour rappel, voici notre plan IP :

Une image contenant texte, diagramme, capture d’écran, ligne

Description générée automatiquement



Dans cette tâche, on a mis en place un VPN SSL afin que des utilisateurs distants puissent accéder de manière sécurisée aux ressources interne de l’entreprise A. Le client sera donc dans le réseau de l’entreprise B. les communications entre le firewall A et le client seront encapsulé et protégé via un tunnel TLS chiffré.

En ce qui concerne les utilisateurs, j’ai gardé l’annuaire LDAP déjà créé pour la tache 4

Une image contenant texte, capture d’écran, logiciel, Icône d’ordinateur

Description générée automatiquement

Et j’y ai ajouté un utilisateur afin qu’il puisse s’authentifier :

Une image contenant texte, capture d’écran, logiciel, Icône d’ordinateur

Description générée automatiquement

L’utilisateur que l’on va utiliser par la suite pour s’authentifier est vpn\_ssl\_user. Ici, on retrouve les informations de notre nom de domaine d’annuaire LDAP (encadré en rouge)

Une fois l’annuaire et l’utilisateur mis en place, il a fallu que je mette en place une politique d’authentification. J’ai configuré celle-ci de façons à ce que l’authentification se fasse avec l’annuaire LDAP en utilisant les identifiants d’utilisateurs.

Une image contenant texte, capture d’écran, logiciel, Icône d’ordinateur

Description générée automatiquement

Ensuite, j’ai configuré le portail captif pour que la correspondance entre l’authentification et l’interface se fasse entre l’annuaire LDAP interne et l’interface OUT (puisque les connexions VPN viennent de l’extérieur)

Une image contenant texte, capture d’écran, logiciel, Icône d’ordinateur

Description générée automatiquement

Aussi, il faut attribuer des droits d’accès pour que le VPN SSL fonctionne donc j’ai autorisé l’accès VPN, mais seulement pour la politique de VPN SSL :

Une image contenant texte, capture d’écran, logiciel, Icône d’ordinateur

Description générée automatiquement

Jusqu’ici, nous avons configurer l’authentification au pare-feu. Une fois cela fait, il faut activer et configurer le service VPN SSL.

Une image contenant texte, logiciel, Icône d’ordinateur, Page web

Description générée automatiquement

Une image contenant texte, logiciel, Icône d’ordinateur, Page web

Description générée automatiquement

Une image contenant texte, logiciel, Icône d’ordinateur, Page web

Description générée automatiquement

(Détailler la config)

Enfin, ma configuration du VPN est fini, mais il faut configurer la politique de filtrage, afin qu’on autorise ou refuse certain paquet provenant de vpnssl\_udp et vpnssl\_tcp.

Une image contenant texte, capture d’écran, logiciel, Icône d’ordinateur

Description générée automatiquement

Ou bien encore configurer une translation d’adresse si l’on souhaite que le client accède à internet.

Une image contenant texte, capture d’écran, logiciel, Icône d’ordinateur

Description générée automatiquement

Installation openvpn connect sur le client et configuration :

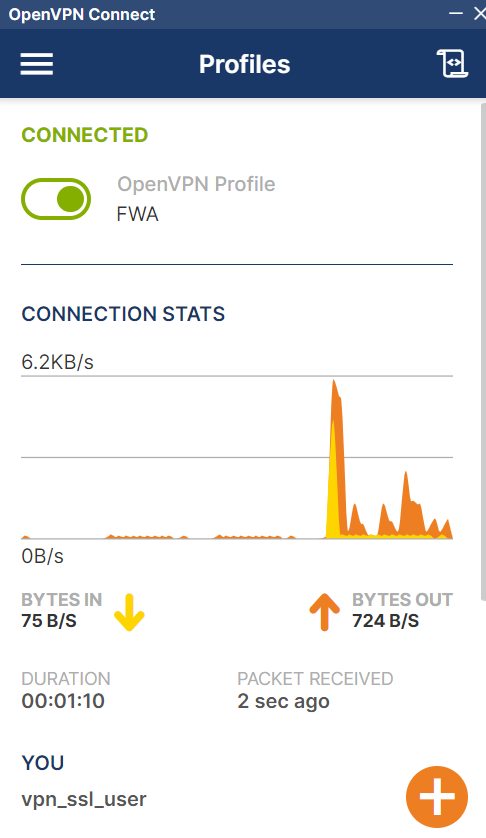
On importe le fichier de configuration du VPN (format .ovpn). Puis on entre les identifiants :

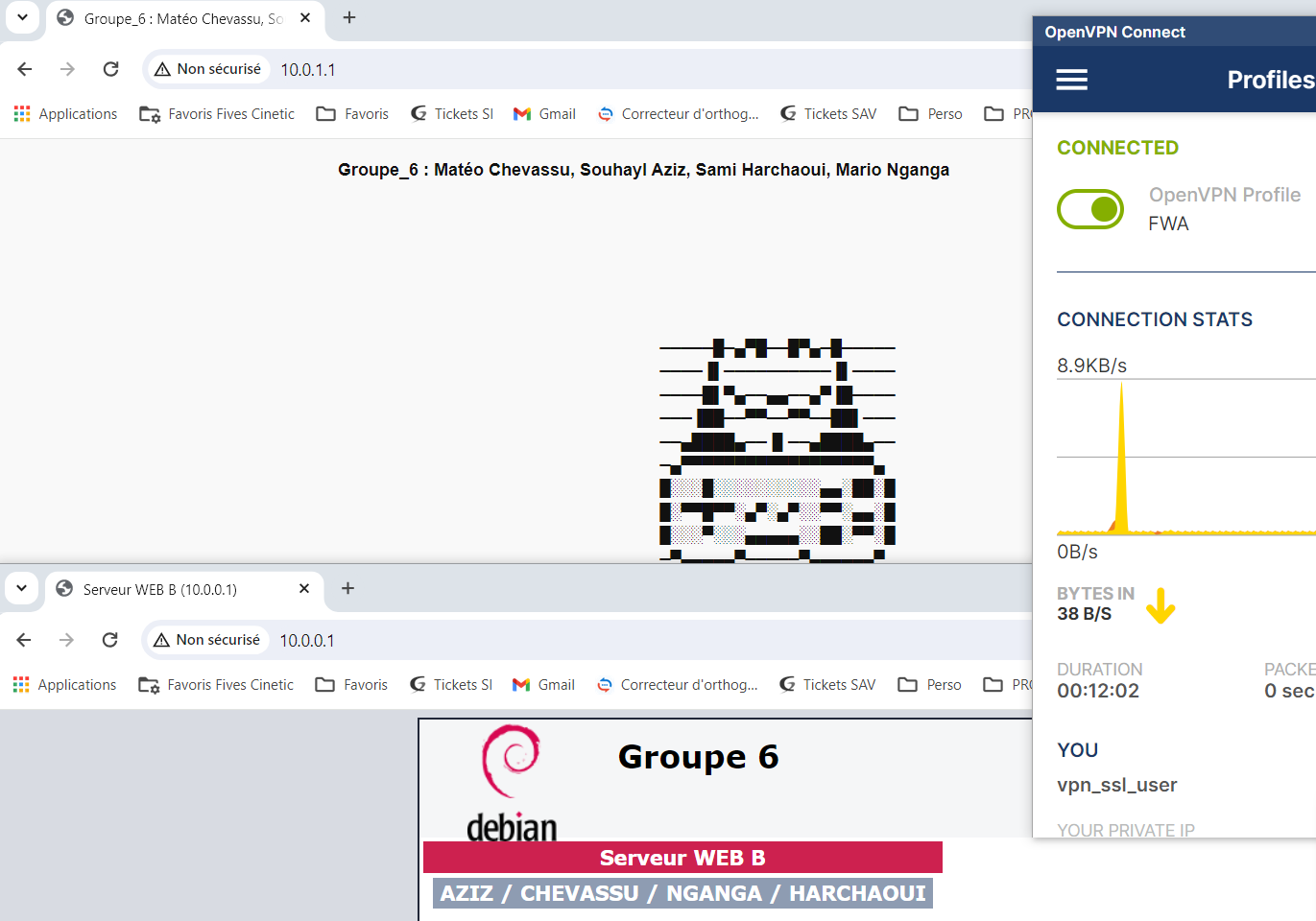
Une image contenant texte, capture d’écran, Police, nombre

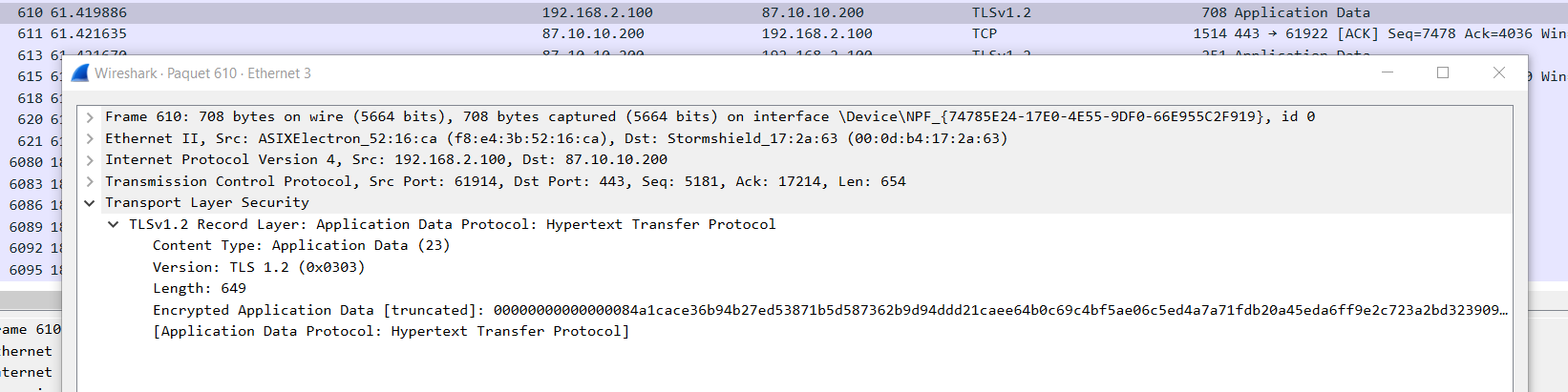
Description générée automatiquement

On retrouve l’@IP du firewall distant, et l’utilisateur créé avant (vpn\_ssl\_user)

Test :







On voit que nos paquets sont encapsulé dans une couche TLS (1.2).  
Aussi,