08/01/2018

Léo Guilpain & Legris Thomas

Mise en place de VPN avec IPSec

[Sous-titre du document]

Table des matières

[Introduction 2](#_Toc502779853)

[Mise en place de 2 sites 2](#_Toc502779854)

[Mise en place d’un tunnel IPSec en AH 3](#_Toc502779855)

[Travail à réaliser 3](#_Toc502779856)

[Mise en place sur GNS3 4](#_Toc502779857)

# Introduction

Le but de ce TP est de relier deux sites d’une même entreprise à l’aide d’un tunnel sécurisé par IPSEC. On utilisera dans un premier temps le protocole AH (pas de chiffrement) puis le protocole ESP (chiffrement des données) à clé manuelle.

Ensuite, il faudra mettre en place le protocole IKE pour échanger les clés. On l’utilisera d’abord avec des clés partagées puis avec des clés publique RSA.

# Mise en place de 2 sites

Une image contenant carte, texte

Description générée avec un niveau de confiance très élevé

Dans un premier temps, nous avons réalisé la commande :

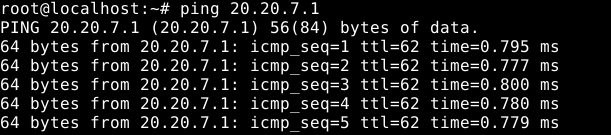
*Router(config)#ip route 20.20.7.0 255.255.255.0 30.30.30.7*

Cette commande permet d’ajouter une route statique entre les deux routeurs. Les commandes sont réalisées de chaque côté.

Ensuite nous avons ajouté la route par défaut suivante :



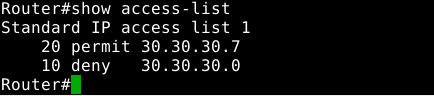
D’après la capture ci-dessus, nous voyons que la connectivité se fait bien. Nous arrivons à pinger la machine voisine.



# Mise en place d’un tunnel IPSec en AH

## Travail à réaliser

On réalise différents ACL permettant de gérer les différents accès. En réalisant la commande « *show access-list »* on peut voir les ACL présentes.



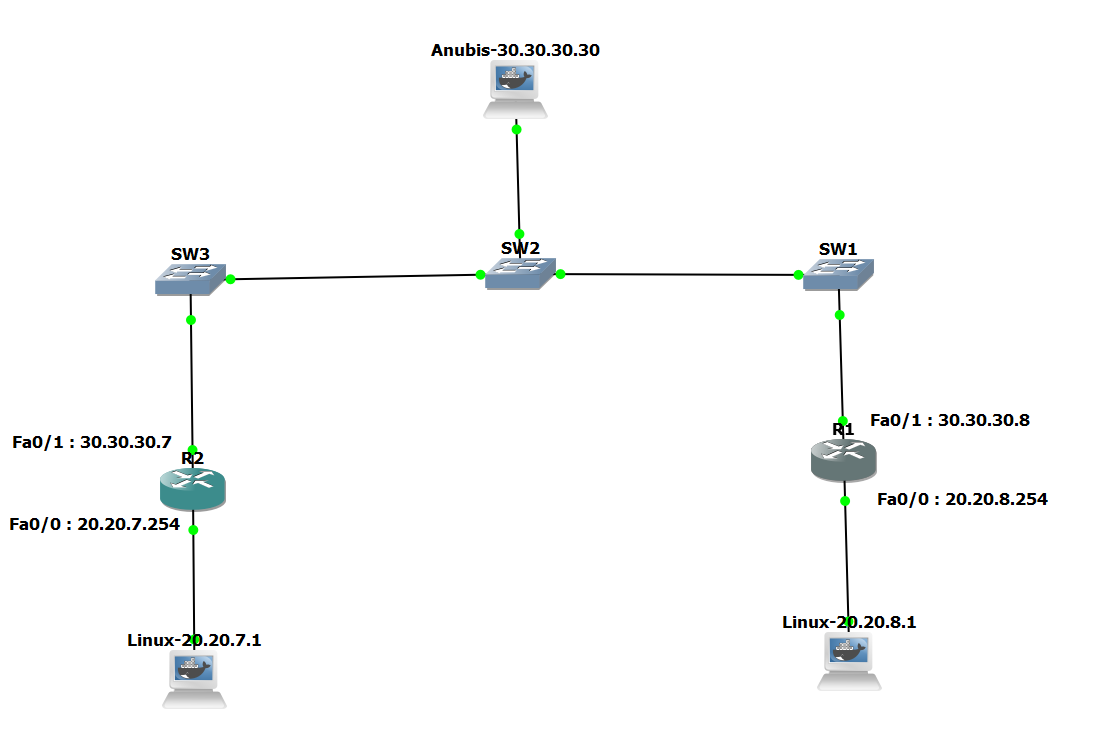
On met en place les différentes combinaisons possibles de protocoles et algorithmes utilisables dans les transform set. Comme vous pouvez le voir ci-dessous, notre transform set se nomme tunnel. Les règles sont définies par les ACL et un mot de passe 0123456789 répété 3 fois.



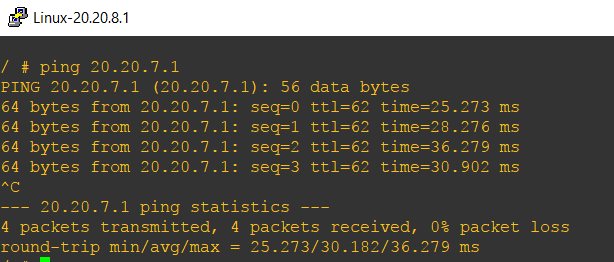
Ensuite nous avons suivi la procédure pour créer un tunnel IPsec avec clefs manuelles : 

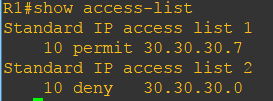
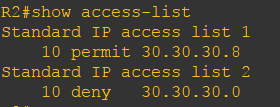


Mise en place sur GNS3

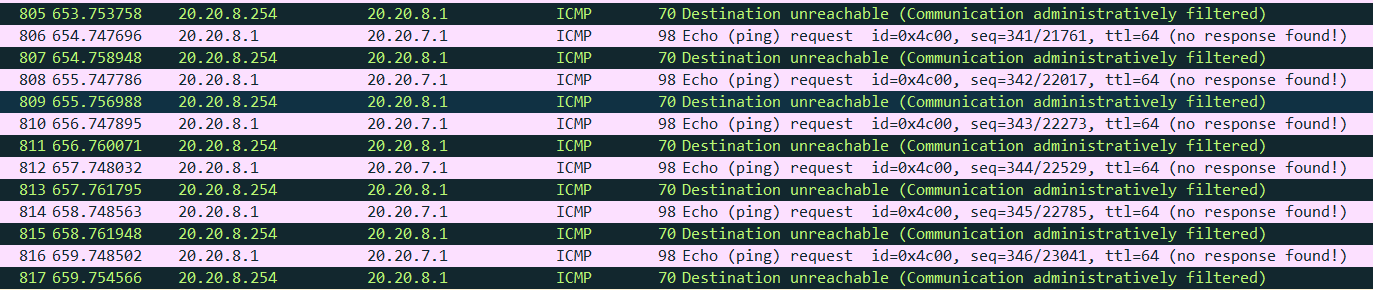


Après avoir attribué les différentes adresses aux différents postes, on peut voir que la connectivité se fait correctement :

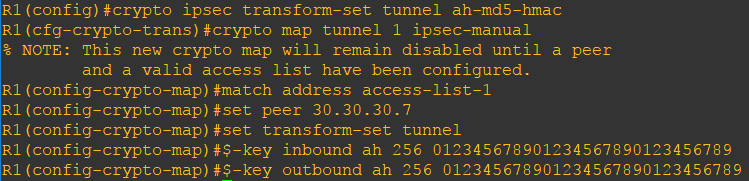


Ensuite, on a mis en place différents ACL.

Après avoir mis en place les ACL, on obtient :

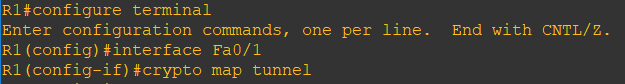


On met en place les différentes combinaisons possibles de protocoles et algorithmes utilisables dans les transform set. Idem que précédemment, le transform set se nomme tunnel et nous avons créé une map nommé tunnel également. Les mots de passe sont similaires et nous allons nous relier au poste 30.30.30.7.



On réalise ceci sur les deux routeurs.

Ensuite, on l’applique à l’interface sur lequel le tunnel est utilisé.



Conclusion

Dans ce TP nous avons tenté de mettre en place un tunnel. Cependant, nous n’avons pas réussi à le faire fonctionner. On peut voir que les paquets sont filtrés, ce sont les ACL qui posent problème.