03/11/2017

Léo Guilpain & Thomas Legris

*« J’atteste que ce travail est original, qu’il indique de façon appropriée tous les emprunts, et qu’il fait référence de façon appropriée à chaque source utilisée. »*

Compte rendu TP2

Filtrage d’accès

Table des matières

[Introduction 2](#_Toc497739550)

[Partie 1 : Travail sur le logiciel GNS3 3](#_Toc497739551)

[Fermez tous les accès sur les 3 interfaces de votre routeur 3](#_Toc497739552)

[Restriction sur le ping 5](#_Toc497739553)

[Partie 2 : Mise en pratique sur un réseau réel 6](#_Toc497739554)

[Fermez tous les accès sur les 3 interfaces de votre routeur 7](#_Toc497739555)

[Restriction sur le ping 8](#_Toc497739556)

[Conclusion 9](#_Toc497739557)

# Introduction

Après avoir vu deux techniques de piratages lors du premier TP, nous devons maintenant établir des règles de filtrages en fonction d’un cahier des charges bien précis. Ce TP est composé de 2 parties : tout d’abord, l’élaboration du filtrage grâce au logiciel GNS3, permettant la virtualisation d’un réseau, puis la mise en pratique du filtrage sur des machines réels et des vrais routeurs Cisco.

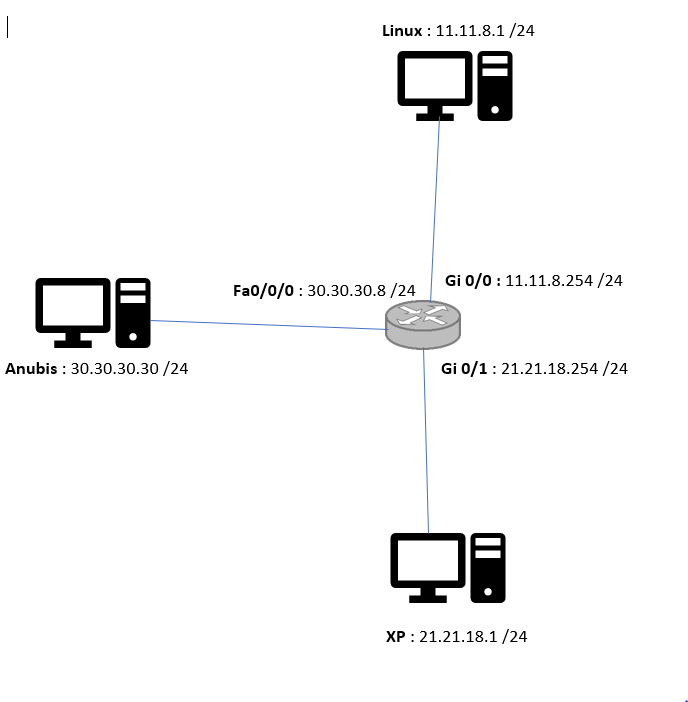


Figure 1 : Schéma utilisé pour notre TP

# Partie 1 : Travail sur le logiciel GNS3

Une image contenant ciel, carte, texte

Description générée avec un niveau de confiance élevé

Figure 2 : Réseau GNS3

Après avoir mis en place ce réseau ainsi que les routes par défaut, on vérifie si les machines appartenant à des réseaux différents peuvent se pinger. Pour cela, la machine 21.21.1.1 va pinger la machine 30.30.30.30 et la machine 11.11.1.1 :

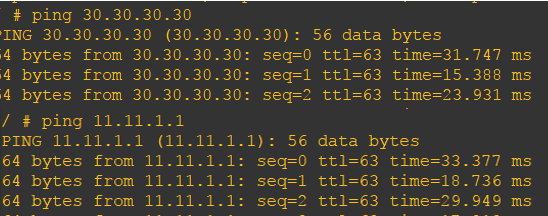


Figure 3 : Ping entre les différentes machines

On peut voir que les machines peuvent toutes se pinger.

Après avoir vérifié que toutes les connexions fonctionnent, on va devoir répondre aux contraintes du cahier des charges.

## Fermez tous les accès sur les 3 interfaces de votre routeur

On a bloqué les trois interfaces du routeur en filtrant les entrées de chacune d’elles. Ainsi on peut voir que le flux est bien filtré puisque les machines ne peuvent plus se pinger.

D’après la capture Wireshark, on peut voir que l’action request a bien été faite contrairement à l’action reply qui n’a pas été effectuée.

Le filtrage n’est pas fin, il faut filtrer un peu plus finement afin de laisser passer les Reply.

Une image contenant texte

Description générée avec un niveau de confiance élevé

Figure 4 : Blocage de l'interface Fa0/0

Grâce à cette commande on a bloqué l’interface Fa0/0 en filtrant l’entrée du routeur. On fait de même pour toutes les interfaces.

Une image contenant texte

Description générée avec un niveau de confiance très élevé

Figure 5 : show access-lists

Après avoir fermé les accès, on refait un ping pour vérifier :

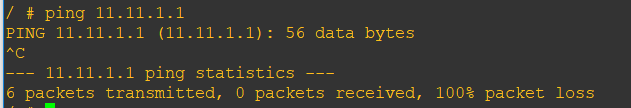


Figure 6 : Ping vers 11.11.1.1

On peut voir que les paquets ne sont pas transmis et donc que les interfaces sont bien fermées.

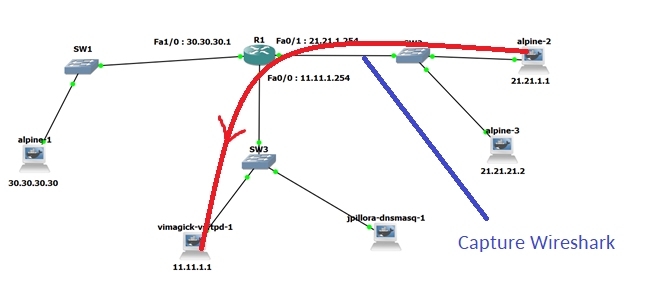


Figure 7 : Schéma montrant les actions effectuées

On obtient ce résultat sur la capture : Une image contenant moniteur, capture d’écran, mur, montrant

Description générée avec un niveau de confiance très élevé

Figure 8 : Observation du filtrage sur le réseau

On voit bien que le request se fait bien. En revanche, il y a un problème sur le reply.

Dans la suite, une nouvelle contrainte s’ajoute, c’est-à-dire qu’il ne faut pas filtrer le reply.

## Restriction sur le ping

On a utilisé la commande :

Une image contenant périphérique, objet

Description générée avec un niveau de confiance élevé

Figure 9 : Commande pour filtrer plus finement

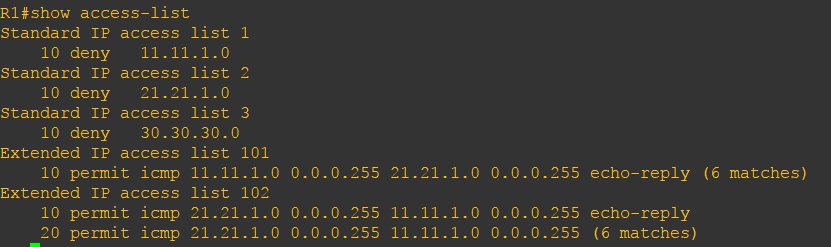


Figure 10 : Nouvelle contrainte sur le reply

On refait ensuite une capture Wireshark au même endroit, on obtient ceci :

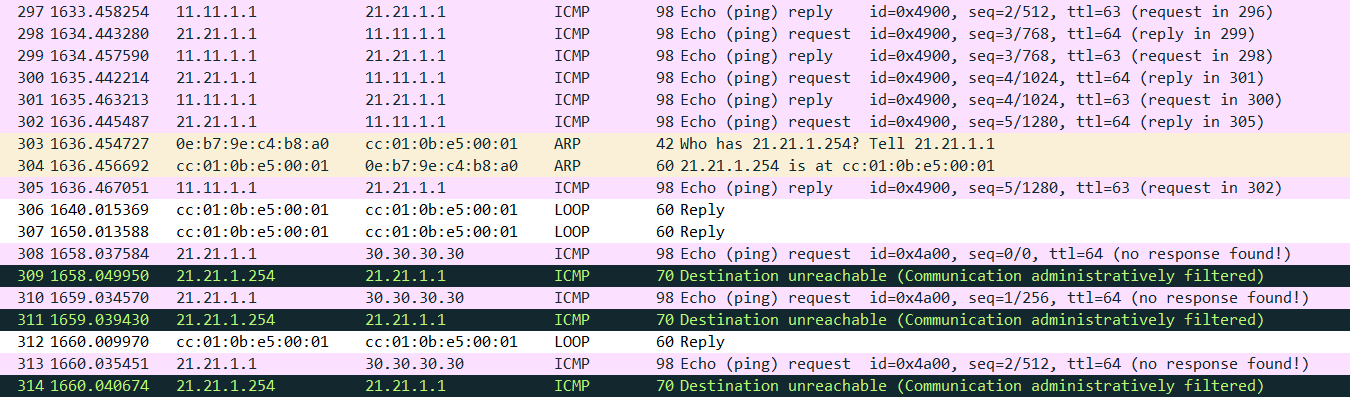


Figure 11 : Observation du trafic suite à la nouvelle contrainte

On voit bien sur cette capture que dorénavant le « reply » n’est plus filtré lorsque la machine 21.21.1.1 ping la machine 11.11.1.1. En revanche, comme on peut le voir, lorsque la machine 21.21.1.1 tente de pinger la machine 30.30.30.1 le reply est toujours filtrer.

# Partie 2 : Mise en pratique sur un réseau réel

La figure suivante représente l’architecture que nous allons utiliser lors de ce Tp, elle fait référence à la figure présente en introduction.

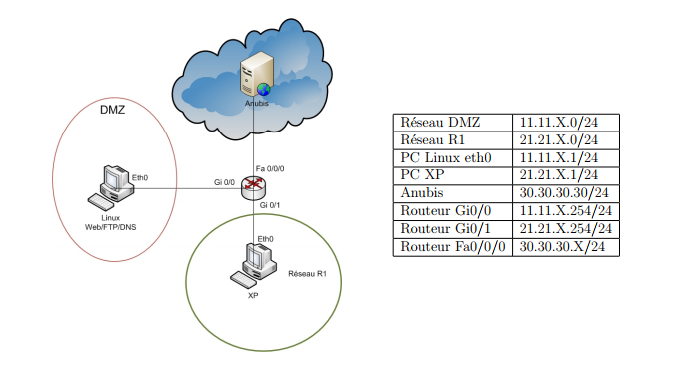


Figure 12 : Architecture du réseau et adressage des différents équipements

La première étape est de configurer les routeurs et les machines, l’adressage, l’établissement des routes entres les machines.

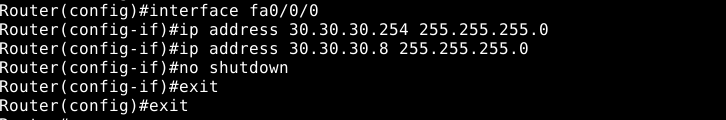


Figure 13 : Configuration d’une interface du routeur

Pour vérifier le bon fonctionnement du réseau nous allons réaliser des pings entre les machines :

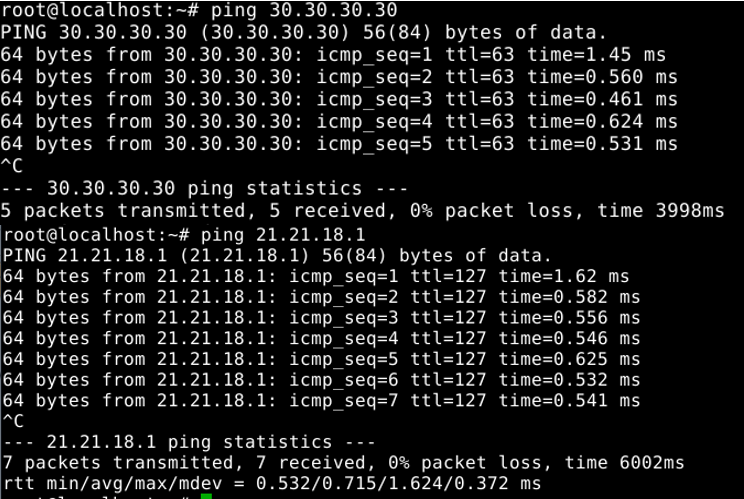


Figure 14 : Ping entre les machines

Comme dans la première partie, la configuration du réseau est bien fonctionnelle, les machines peuvent envoyer des données à travers le réseau, il n’y a aucun filtrage actuellement.

## Fermez tous les accès sur les 3 interfaces de votre routeur

Nous avons tous d’abord fermer les accès en entrée sur chaque interface du routeur :

* Fa0/0/0
* Gi0/0
* Gi0/1

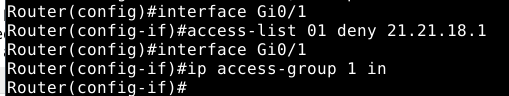


Figure 15 : Fermeture de l’interface Gi0/1

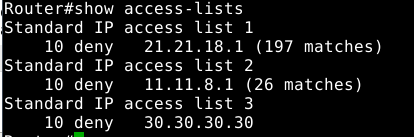


Figure 16 : Récapitulatif des 3 interfaces fermées

On peut voir que les pings entre les 2 réseaux sont bien filtrés :

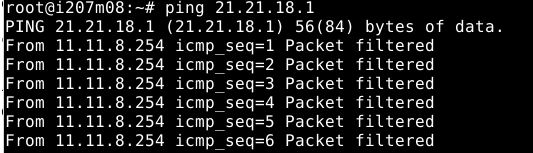


Figure 17 : Ping filtrés

La prochaine étape va être d’affiner notre cahier des charges.

## Restriction sur le ping

On doit donc filtrer les pour que seules le réseau R1 accède au réseau DMZ :

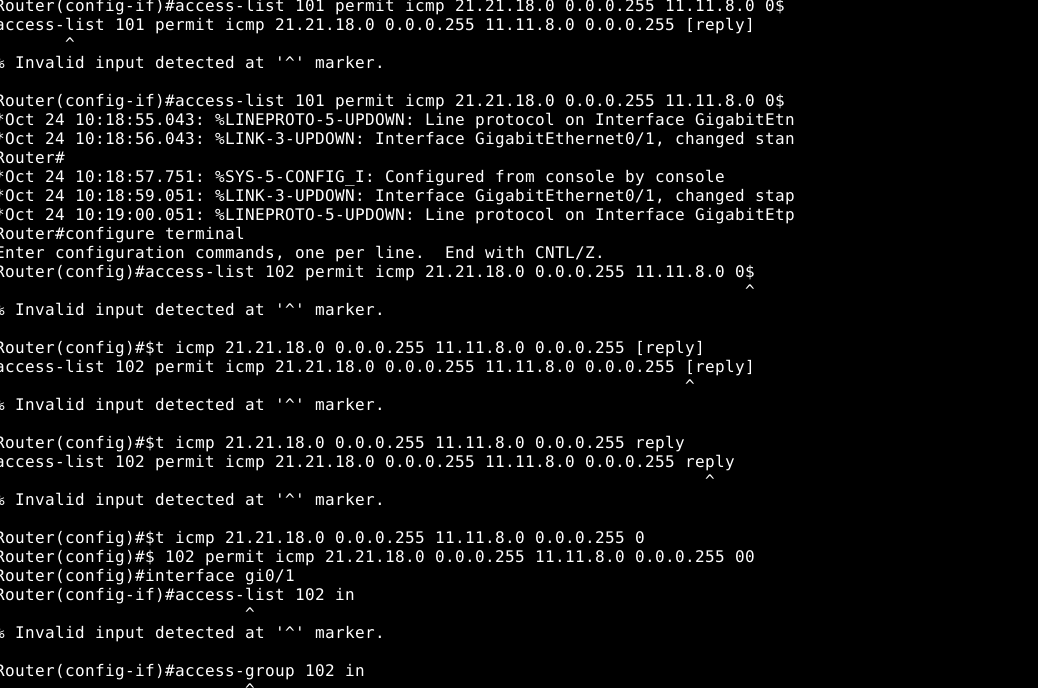


Figure 18 : Commande permettant ce filtrage

# Conclusion

Les 2 séances de TP nous ont permis de manipuler de manière virtuelle et pratique les règles de filtrages, standard et étendues. Nous avons d’abord interdit tous les accès, puis nous avons affiné notre filtrage en autorisant certaines machines à accéder à d’autres. Malheureusement, nous n’avons pas pu finir le TP pratique, et donc avancer plus loin dans le cahier des charges.