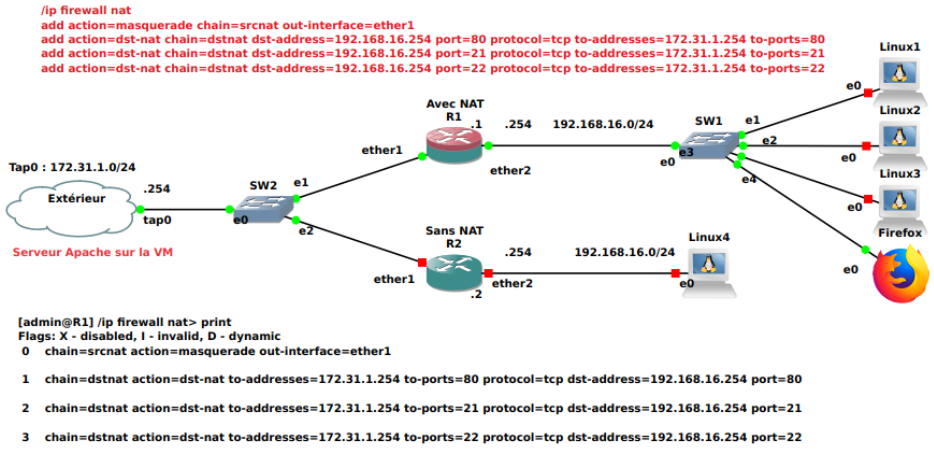
UNIVERSITÉ CAEN NORMANDIE

TP NAT-2

31.01.2023

On masque les @IP privées le retour ☺

Auteur : Pascal Fougeray



Source : Moi ☺

1 Préambule

— Ce TP peut être fait chez vous, il n'y a aucune difficulté majeure, il ne va pas vous occuper 2h30 !☺
— Ce TP utilise deux routeurs,
  — L'un fait du NAT et **masque** un serveur Web
  — L'autre pas.
— Il doit être fait après le TP LAMP, si fait avant juste sur la VM lancer : ***apt install apache2***
— On travaille dans la VM et qu'avec les logiciels GNS3 et Wireshark
— On va installer
  — dans GNS3 un navigateur web : **Firefox 31.1.1~2 qui fonctionne avec *vncviewer***
  — sur la VM *vncviewer* : ***apt install xtightvncviewer*** du moins je pense
— Vous devez vous rappeler ce que donne un serveur DHCP à un client.
— **Prenez des notes sur ce que vous comprenez, ces notes vous y aurez le droit de les avoir avec vous au CT !**

2 Introduction

Dans ce TP, je vous propose de **voir** :
— Les adresses IP publiques et privées
— Le principe du NAT pour cacher un serveur ici ce sera le serveur Web.
— etc...

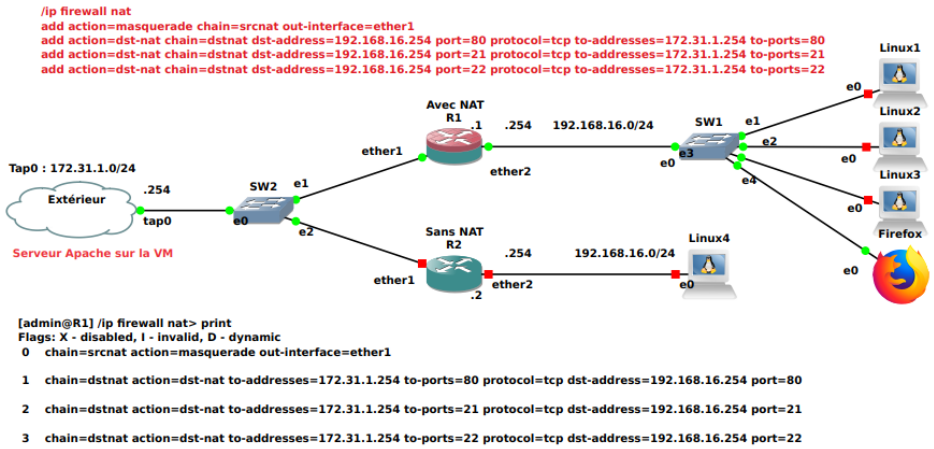
3 L'étude théorique

1. Quelle est l'adresse IP **privée** du serveur Web de la Fac www.unicaen.fr ?
2. Quelle est l'adresse IP **publique** du serveur Web de la Fac www.unicaen.fr ?

3. Où se trouve ce serveur Web ?
4. Pourquoi est-ce que l'on procède comme cela ?

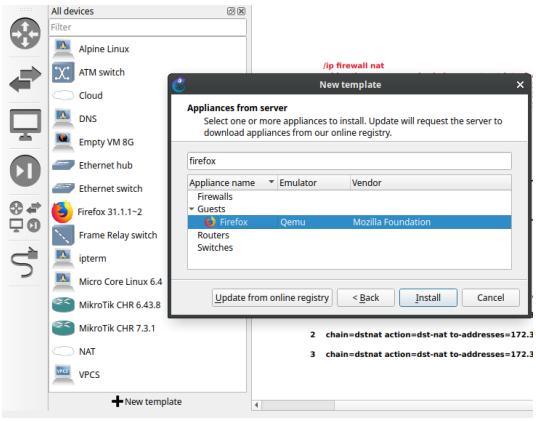
4 L'étude pratique

On va travailler sur cette structure

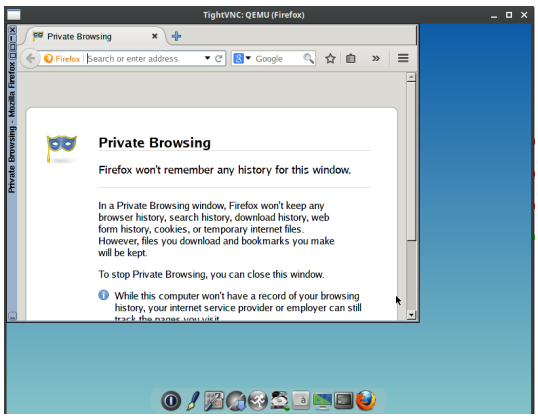


Pour se loguer sur un routeur, le login est admin et il n'y a pas de MDP donc on valide

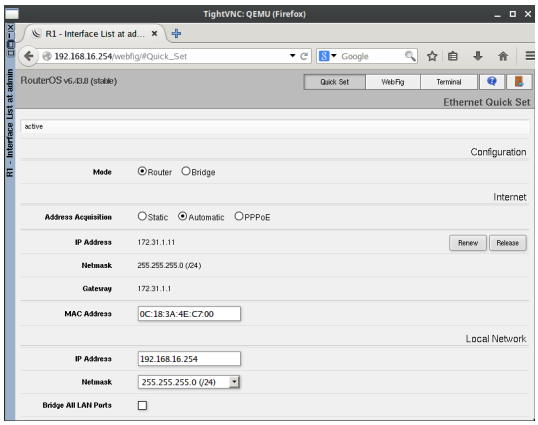
1. **Récupérez** sur ecampus le Projet **TP-NAT-2-le-retour**
2. **Ouvrez**-le dans GNS3
   Si ça ne marche pas c'est parce que l'***appliance firefox*** n'est pas installé dans GNS3. On va le faire
3. Dans GNS3, là où l'on choisi les composants à mettre, **faites *new template et installez firefox***



   Une fois l'***appliance firefox*** installée correctement vous devez pouvoir ouvrir le projet **TP-NAT-2-le-retour**
4. **Lancez** toutes les machines**.**
5. **Ouvrez** une console avec firefox
   Vous devriez obtenir quelque chose comme cela.
   Oui, oui, un Linux avec cette fois-c une interface graphique qui tient dans même pas 100Mo... et qui n'a besoin que de 256Mo de RAM pour fonctionner ☺



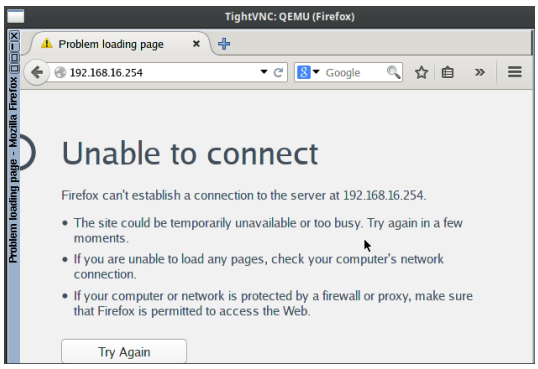
6. **Saisissez** comme URL, l'@IP de l'interface Ethernet ether2 du routeur R1, ce doit être 192.168.16.254 ?
   Vous devriez obtenir quelque chose comme cela



7. Sur R1, **lancez** la commande ***/ip service print***
   Vous devriez obtenir quelque chose comme cela. On voit les ports ouverts et les services rendus !

```
[admin@R1] > /ip service print
Flags: X - disabled, I - invalid
 #    NAME                                      PORT ADDRESS
 0    telnet                                    23
 1    ftp                                       21
 2    www                                       80
 3    ssh                                       22
 4    www-ssl                                   443
 5    api                                       8728
 6    winbox                                    8291
 7    api-ssl                                   8729
[admin@R1] >
```

8. Maintenant,nous allons devoir
   (a) Soit fermer le serveur Web qui tourne sur le routeur : ***/ip service disable www***
   (b) Soit changer son numéro de port : ***/ip service set www port=100***
   (c) **Choisissez** la seconde solution c'est mieux ! ! !
9. **Vérifiez** que cela fonctionne en rechargeant la page sur firefox.
   Normalement, vous devriez avoir Serveur inaccessible ou un message de ce genre.



Ce qui est logique non ?

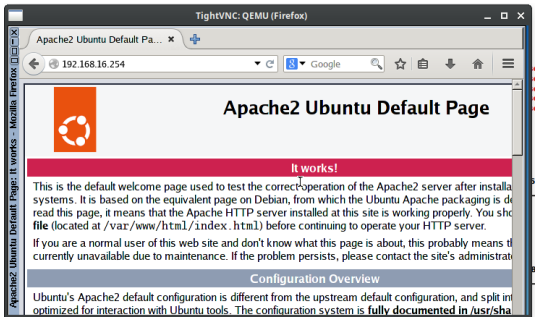
10. Nous allons maintenant faire en sorte que le routeur **transmette** la requête au serveur Web de la VM donc sur l'adresse 172.31.1.254, @IP de Tap0. Il en est de même pour les ports 22 et 21.

    Lancez la commandes suivante sur le routeur R1

    ```
    /ip firewall nat
    add action=dst-nat chain=dstnat dst-address=192.168.16.254 port=80 protocol=tcp
    to-addresses=172.31.1.254 to-ports=80
    ```

11. **Vérifiez** que cela fonctionne en rechargeant la page sur firefox

    Vous devriez obtenir quelque chose comme cela.



    Est-ce logique ?

12. Questions de logique
    (a) À quoi sert le NAT dans cette situation ?
    (b) **Pensez**-vous que votre Box chez vous fait du NAT de cette manière là ?
    (c) **Essayez**, vous relevez son @IP publique, il y a peut être un serveur Web qui tourne sur votre BOX...

        Est-il accessible de l'extérieur ?

        Si oui, pourquoi ne pas accéder à votre propre serveur Web de votre PC.

13. Question plus difficile... Est-ce possible de faire cela avec les ports DHCP 67 et 68 ?

14. Vous avez terminé ?

    Faites en sorte que cela fonctionne avec le protocole SSH ☺

    il vous faudra installer une nouvelle appliance nommée ip-term qui démare encore plus vite qu'un micro-Linux

5 Conclusion

On a vu au TP précédent que le NAT a permis qu'avec pas assez d'@IP on connecte beaucoup de gens avec une seule IP ! ! !

Le NAT a aussi permis de masquer des serveurs derrière un routeur, en réalité ce n'est pas un routeur mais une machine spéciale pour la protection d'un site appelé **FireWall** (Oui oui Mur de feu)

Si vous allez en Master option sécurité vous en apprendrez plus dans ce domaine.

Chaque paquet IP que vous envoyez sur internet a un identifiant et c'est cet identifiant qui permet de savoir si c'est Pierre, Paul ou Jacques qui a contacté tel ou tel serveur !