Semaine 7 – NAT, filtrage

Exercice 1

Cette question utilise principalement votre machine hôte.

1. Démarrez un navigateur Web et connectez-vous sur http://ip.lafibre.info.
   — quelle est votre adresse IPv4 telle que détectée par le site distant ?
   — quelle est l'adresse IPv4 de votre carte réseau ? (si votre machine hôte est un Unix classique, utilisez `ifconfig`, si c'est un Linux et que `ifconfig` n'est pas installé, utilisez `ip addr`, si c'est un Windows, cliquez 65433268 fois pour trouver votre adresse dans les menus)
   — ces deux adresses sont-elles identiques ? Si non, pourquoi ?
2. Si, comme c'est vraisemblable, les deux adresses ne sont pas identiques, recommencez l'expérience en capturant les paquets avec `wireshark`. Les numéros de port TCP détectés dans la capture et par le site distant sont-ils identiques ? Si non, pourquoi ?
   Note : pour identifier le flux vers `ip.lafibre.info`, vous pouvez vous servir de son adresse IPv4 (46.227.16.8).
3. Si les deux adresses du premier point sont identiques, recommencez l'expérience (points 1 et 2) à l'intérieur d'une machine virtuelle.

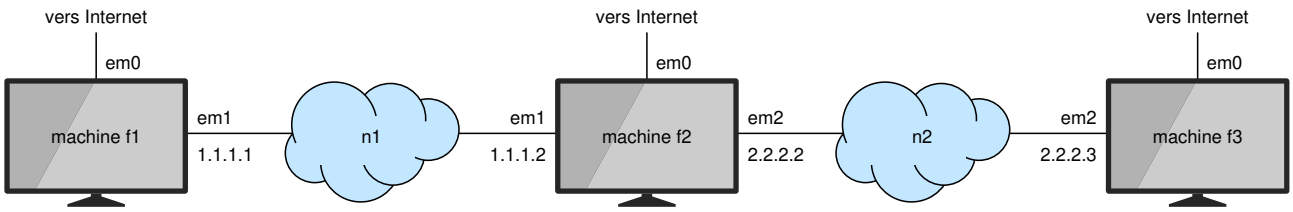
Exercice 2

Démarrez à présent une machine virtuelle `f1`.

1. Démarrez deux captures de trafic avec `wireshark` : la première dans la machine virtuelle sur l'interface `em0`, et la deuxième dans la machine hôte sur l'interface réseau.
2. Comparez les adresses IPv4 et les ports TCP utilisés dans cette connexion.
3. Faites un schéma avec les différentes transformations de paquets opérées sur le chemin.

Exercice 3

Reprenez la topologie à 3 nœuds :



On désire maintenant que le routeur devienne un « garde-barrière », c'est-à-dire qu'il filtre les paquets entre les deux réseaux. Pour tester ce filtrage, nous utiliserons `ping` et `ssh` : démarrez le serveur SSH sur les 3 machines.

1. Configurez la topologie décrite, et testez la connectivité entre `f1` et `f3` avec `ping` et `ssh` (rappel : avec `ssh` on se contente d'aller jusqu'à l'invite du mot de passe, sans chercher à aller plus loin)

2. L'outil mis en œuvre sur `f2` dans cette question et la suivante est PF (pour *Packet Filter*) : il s'agit d'un outil extrêmement puissant. Le but ici n'est pas d'étudier sa configuration en détail [1], mais de comprendre les effets du filtrage.

   La configuration se fait dans le fichier `/etc/pf.conf` que vous pouvez modifier avec l'éditeur de texte de votre choix [2]. Dans un premier temps, créez un fichier `/etc/pf.conf` vide et exécutez la commande `sudo service pf forcestart` pour activer PF.

   Par la suite, après toute modification du fichier, exécutez `sudo pfctl -Fa -f/etc/pf.conf` pour recharger les règles.

3. Vérifiez que l'activation de PF sur `f2` ne modifie pas la connectivité entre `f1` et `f3`.

4. Il peut être utile de démarrer `wireshark` sur `f1` et `f3` pour suivre les paquets à la trace.

5. Les règles de PF sont parcourues de la première à la dernière. À moins qu'une règle n'ordonne un arrêt prématuré de cette séquence, c'est la dernière règle trouvée qui s'applique.
   Entrez les règles suivantes [3] dans `/etc/pf.conf` :

   ```
   # "normaliser" le trafic entrant sur em2 (ex: défragmenter les paquets)
   scrub in on em2 all fragment reassemble

   # bloquer tout le trafic entrant sur em2
   block in on em2 all

   # autoriser ICMP
   pass on em2 inet proto icmp all
   ```

   Avez-vous pensé à recharger les règles ?

   Testez la connectivité avec `ping` et `ssh`. Dans chaque cas, quelle règle s'applique ?

6. Ajoutez une règle pour permettre à `f3` de faire un `ssh` vers `f1` :

   ```
   # autoriser le trafic SSH vers f1
   pass in on em2 inet proto tcp from 2.0.0.0/8 to 1.1.1.1/32 port 22
   ```

   Où cette règle doit-elle être placée ?

   Testez la connexion SSH vers `f1`.

7. PF étant un système de filtrage à états, il maintient une liste des connexions actives. Alors que la connexion SSH précécdente est toujours active (si besoin est, relancez-la), consultez les états maintenus par PF avec `sudo pfctl -s states`.

8. Avec la règle ci-dessus, vous ne pouvez pas faire de connexion SSH de `f1` vers `f3`. Vérifiez. Expliquez pourquoi.

9. Ajoutez une règle pour permettre cette connexion.

1. Vous pouvez consulter https://www.freebsd.org/doc/en_US.ISO8859-1/books/handbook/firewalls-pf.html si vous voulez en savoir plus.
2. Seul `vi` est installé par défaut, mais vous pouvez installer d'autres éditeurs de texte avec la commande `pkg` (à exécuter avec `sudo`).
3. Les commentaires peuvent être omis dans le fichier.