Filtrage réseau avec netfilter/iptables

Philippe Latu
philippe.latu(at)inetdoc.net

https://www.inetdoc.net

Résumé

Ce support de travaux pratiques est une introduction au filtrage réseau. Il reprend la topologie Hub & Spoke des autres supports de la série. Les questions débutent par l'identification des outils et passent à l'application des règles de filtrage avec et sans suivi de communication (stateful vs stateless inspection). On introduit aussi les fonctions de traduction d'adresses (NAT).

Table des matières

1. Copyright et Licence

1.1. Méta-information

Cet article est écrit avec DocBook XML sur un système Debian GNU/Linux. Il est disponible en version imprimable au format PDF : `interco.netfilter.q.pdf`.

Toutes les commandes utilisées dans ce document ne sont pas spécifiques à une version particulière des systèmes GNU/Linux. C'est la distribution Debian GNU/Linux qui est utilisée pour les tests présentés. Voici une liste des paquets contenant les commandes :

- procps - utilitaires pour le système de fichiers /proc
- iproute2 - outils de contrôle du trafic et du réseau
- ifupdown - outils de haut niveau pour configurer les interfaces réseau
- iputils-ping - outils pour tester l'accessibilité de noeuds réseaux
- iputils-tracepath - Tools to trace the network path to a remote host

- hping3 - Active Network Smashing Tool
- thc-ipv6 - The Hacker Choice's IPv6 Attack Toolkit
- iptables - outils d'administration pour le filtrage de paquets et le NAT
- iptstate - top-like interface to your netfilter connection-tracking table
- conntrack - programme pour modifier les tables conntrack

1.2. Conventions typographiques

Tous les exemples d'exécution des commandes sont précédés d'une invite utilisateur ou prompt spécifique au niveau des droits utilisateurs nécessaires sur le système.

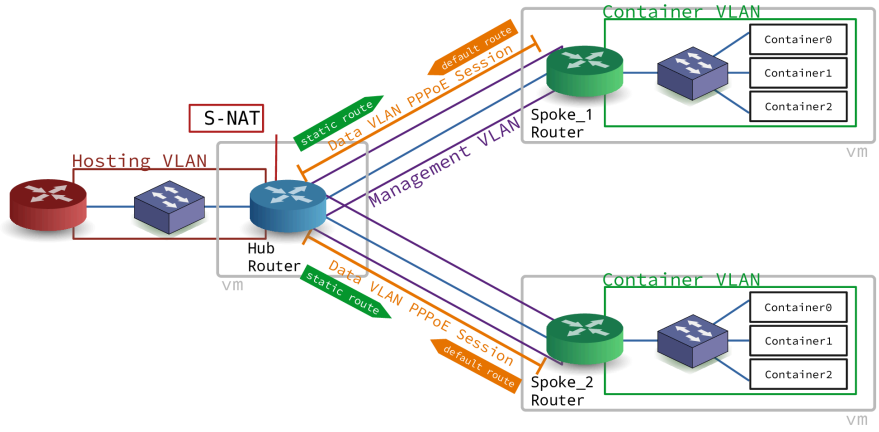
- Toute commande précédée de l'invite `$` ne nécessite aucun privilège particulier et peut être utilisée au niveau utilisateur simple.
- Toute commande précédée de l'invite `#` nécessite les privilèges du super utilisateur.

Le recours aux commandes grep et fmt sert à optimiser la quantité et l'espace occupés dans les copies d'écran données en réponse aux questions. Tous les “tubes“ utilisés pour les copies d'écran peuvent être supprimés de façon à afficher toutes les informations sur un espace qui occupe toute la largeur de la console.

2. Architecture réseau étudiée et filtrage

Les manipulations sur le système de filtrage réseau présentées ici s'appuient sur la topologie Hub and Spoke étudiée dans le support précédent de la série : Topologie Hub & Spoke avec le protocole PPPoE.

La topologie étudiée associe trois routeurs qui ont deux rôles distincts.



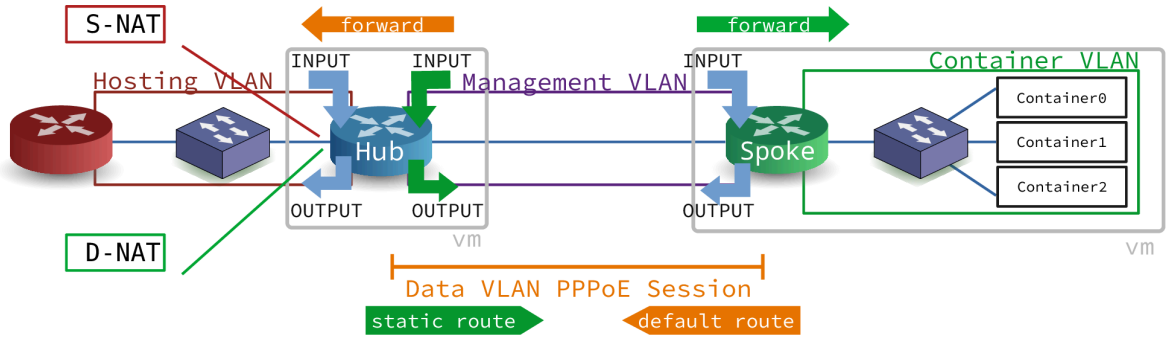
Topologie entre deux routeurs Hub et Spoke avec PPPoE

Routeur central, Hub, Broadband Remote Access Server, BRAS

> Ce routeur réalise une interconnexion LAN/WAN. Il fournit un accès Internet aux routeurs de sites distants via ses interfaces WAN. Il dispose de son propre accès Internet via son interface LAN.

Routeur d'extrémité, Spoke, Customer Premises Equipment, CPE

> Ce routeur réalise aussi une interconnexion LAN/WAN. À la différence du routeur Hub, il obtient l'accès Internet sur son interface WAN et il met cet accès à disposition d'un réseau local de site représenté par des conteneurs LXD.



Topologie Hub & Spoke et filtrage

Routage et traduction d'adresses (situation de départ)

Les manipulations qui suivent supposent que la topologie Hub & Spoke est en place et fonctionnelle. On s'appuie sur le support précédent de la série : Topologie Hub & Spoke avec le protocole PPPoE

- Le routeur Hub doit s'assurer que le trafic réseau qu'il route vers et depuis l'Internet correspond bien au plan d'adressage défini. Dans ce but, il attribue les adresses du lien point à point ainsi qu'une route statique à destination du réseau d'extrémité distant.

  Le routeur Hub assure la traduction des adresses sources du réseau distant vers l'Internet.

- Le routeur Spoke doit obtenir son adresse IPv4 de réseau étendu via PPP et assurer le routage de son réseau local. Il dispose d'une route par défaut qui désigne le lien point à point comme seul accès vers l'Internet.

Les questions ci-dessous ont pour objectif de valider le fonctionnement du routage et de la traduction des adresses sources en sortie du routeur Hub vers l'Internet.

Q1. Comment tracer le chemin suivi par les paquets IPv4 et IPv6 d'un conteneur à un autre conteneur du site distant de l'autre branche de la topologie ?

Rechercher le paquet contenant la commande tracepath qui permet d'afficher le chemin suivi par le trafic réseau.

Q2. Comment caractériser la traduction d'adresses source en sortie du routeur Hub ?

La fonction de traduction d'adresse entre dans cadre du filtrage réseau et fait appel aux mêmes outils : netfilter/iptables.

Rechercher le paquet qui contient la commande conntrack puis rechercher les options de cette commande qui permettent d'afficher les états des enregistrements de la table NAT.

3. Les outils de filtrage réseau

Sur un système GNU/Linux, les fonctions de filtrage réseau sont réparties entre les espaces mémoire noyau (kernelspace) et utilisateur (userspace). Les fonctions de filtrage réseau sont disponibles sous forme de modules qui sont chargés dynamiquement dans la mémoire du système en cours d'exécution en fonction de la syntaxe des règles de filtrage ajoutées.

Q3. Quel est le paquet le plus important pour les manipulations sur les fonctions de filtrage réseau ?

Rechercher dans la liste des paquets les mots clés tels que `iptables` ou `firewall`.

Q4. Comment visualiser les modules chargés dynamiquement en fonction de l'utilisation des règles de filtrage réseau ?

Utiliser la commande qui sert à lister les modules chargés en mémoire avant et après avoir consulté les tables de filtrage réseau pour la première fois.

Q5. Quels sont les outils de sauvegarde et de restauration des jeux de règles de filtrage réseau fournis avec le paquet iptables-persistent ?

Consulter la liste des fichiers du paquet.

Q6. Comment visualiser les enregistrements d'états de suivi des communications réseau ?

Rechercher la chaîne `conntrack` dans la liste des paquets.

La section «7.2 Les entrées de conntrack» du Tutoriel iptables décrit précisément les différents champs du suivi de communication.

4. Protection de base des routeurs Hub et Spoke

Le but de cette section est de mettre en place le routage avant de passer aux fonctions de filtrage réseau proprement dites. Elle correspond à la vue Topologie PPP et routage.

Voici une liste de fonctions de protection à mettre en œuvre sur tous les types de routeurs.

Protection contre l'usurpation des adresses sources, rpfilter, BCP38

Ces fonctions de protection comprennent une partie noyau ainsi qu'une partie filtrage avec le module `rpfilter` à implanter dans la table `raw` qui assure un filtrage sans état. Voir Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing.

Les tests de validation de ces mécanismes peuvent se faire à l'aide de la commande hping3. Les résultats doivent être visibles aussi bien dans les journaux systèmes que sur les compteurs des règles de la table `raw`. En avant pour la chasse aux martiens !

Protection contre les dénis de services ICMP, module `netfilter limit`

Les routeurs doivent s'assurer que le volume de trafic qui est présenté en entrée est compatible avec un fonctionnement nominal des services.

Protection contre les robots de connexion au service SSH, fail2ban

Les routeurs ont besoin d'un accès d'administration à distance via SSH. Pour autant, cet accès doit être protégé contre les tentatives d'intrusion par dictionnaire de couples d'authentifiants.

L'outil fail2ban fourni avec le paquet du même nom introduit une chaîne de filtrage dédiée à ces tentatives d'intrusion.

4.1. Protection contre l'usurpation d'adresse source

Q7. Comment afficher la liste des règles de filtrage de la table `raw` dédiée au filtrage sans état (stateless) ?

Rechercher dans les pages de manuels de la commande iptables les options relatives aux listes et aux compteurs.

La visualisation des compteurs de correspondance des règles de filtrage est indispensable pour qualifier le fonctionnement du filtrage

Q8. Comment activer la protection contre l'usurpation des adresses sources au niveau du noyau ?

Rechercher les informations relatives à la fonction Reverse Path Forwarding du noyau Linux. Identifier les rôles des 3 valeurs possibles de cette fonction.

La documentation est à cette adresse : Kernel IP sysctl.

Q9. Comment enregistrer les tentatives d'usurpation d'adresses dans les journaux système ?

Rechercher les entrées de l'arborescence `/proc` relatives aux paquets “martiens“.

Rechercher aussi le paramètre relatifs aux “martiens“ dans le fichier `/etc/sysctl.conf`.

Q10. Comment valider la fonction de blocage des tentatives d'usurpation d'adresses entre le routeur Hub et les routeurs Spoke ?

Installer le paquet `hping3` sur le routeur Hub.

Rechercher dans les pages de manuels de la commande hping3 les options qui permettent de générer du trafic ICMP avec des adresses source aléatoires à destination d'un conteneur hébergé sur un routeur Spoke.

Q11. Comment filtrer les tentatives d'usurpation d'adresses source au plus tôt de façon à limiter le coût de traitement de ces paquets falsifiés sur le système ?

Identifier le nom de la table de filtrage sans état et rechercher la fonction associée au filtrage des adresses sources usurpées. Rechercher dans les pages de manuels `iptables-extensions` les informations relatives au module `rpfilter`.

Ajouter une règle spécifique dans la table de traitement sans état pour les protocoles IPv4 et IPv6.

Q12. Comment caractériser les nouvelles règles de filtrage entre le routeur Hub et les routeurs Spoke ?

Pour les tests IPv4, il suffit de reprendre les mêmes tests que ceux effectués plus haut avec la commande hping3.

Installer le paquet `thc-ipv6` sur le routeur Hub pour disposer des outils de tests spécifiques au protocole IPv6.

Rechercher dans les pages de manuels de la commande atk6-thcping6 les options qui permettent de générer du trafic ICMP avec une adresse source falsifiée à destination d'un conteneur hébergé sur un routeur Spoke.

4.2. Protection contre les dénis de service ICMP

Q13. Comment peut-on se protéger contre un nombre de sollicitations ICMP trop important ?

Rechercher dans le guide Tutoriel iptables la correspondance Limit qui permet de définir un seuil au delà duquel les nouveaux flux réseau ne sont plus acceptés.

Il faut ajouter une règle spécifique au protocole ICMP après celle qui assure le traitement des flux déjà enregistrés dans les tables de suivi d'état (Stateful).

Q14. Comment qualifier le fonctionnement des règles de limitation du nombre de nouvelles requêtes ICMP ?

Rechercher les options de la commande hping3 qui permettent de générer des flux ICMP en utilisant des adresses IPv4 source aléatoires.

Attention ! Il faut positionner la politique par défaut en mode "tout ce qui n'est pas autorisé est interdit“ sur le routeur cible le temps du test de qualification.

4.3. Protection contre les robots de connexion au service SSH

Q15. Quel est la fonction du paquet fail2ban ?

Afficher la description du paquet fail2ban après l'avoir installé.

Q16. Quel est le numéro de port utilisé par le service SSH sur les routeurs ?

Il est important de connaître les caractéristiques du service qui doit être surveillé par fail2ban. Rechercher dans la liste des ports réseau ouverts celui qui concerne le service SSH.

Q17. Quel est le fichier de configuration du service SSH qui permet de définir le numéro de port en écoute avec le protocole TCP ?

Repérer le répertoire qui contient les éléments de configuration du service SSH.

Q18. Quels sont les deux fichiers de configuration principaux fournis à l'installation du paquet `fail2ban` ?

Rechercher dans l'arborescence des fichiers de configuration, les informations relatives aux traitements assurés en cas de détection d'erreurs de connexion à n'importe quel service, puis les informations spécifiques au service SSH.

Q19. Comment caractériser le fonctionnement du service fail2ban ?

Si le service a été installé et configuré sur un routeur Spoke, il est possible de lancer plusieurs tentatives de connexion SSH depuis le routeur Hub en se trompant de mot de passe.

On peut alors afficher les règles de filtrage iptables et consulter l'état de la prison fail2ban.

5. Règles de filtrage communes à toutes les configurations

La mise en place du filtrage réseau sur les équipements doit répondre à deux principes.

- On considère que les équipements d'interconnexion mis en œuvre dans ces travaux pratiques délimitent des périmètres de dimension moyenne. Par conséquent, on a une connaissance exhaustive des flux réseaux sur le système. On adopte donc la règle : tout trafic réseau non autorisé est interdit.

- On fait le choix d'un filtrage basé sur le suivi de communication (stateful inspection). On cherche donc à écrire des règles qui décrivent le plus précisément possible le premier paquet qui doit être enregistré dans la table de suivi de communication. Ces règles de description du premier paquet doivent être placées après celle qui laisse passer le trafic qui correspond ou qui est relatif à une communication déjà enregistrée dans les tables.

- Dans le but de simplifier l'étude du filtrage, on fait le choix d'autoriser tous les flux sortants émis par les routeurs Hub et Spoke. On laisse donc la politique par défaut à `ACCEPT` pour les chaînes `OUTPUT` des routeurs.

On commence par afficher les règles actives sur les différents routeurs à l'issue des questions de la section précédente : Section 4, « Protection de base des routeurs Hub et Spoke ».

Attention ! Les noms d'interfaces correspondent à la maquette de test.

- Régles de filtrage IPv4 côté Hub : fichier `/etc/iptables/rules.v4`.

```
#~~~~~~~~~~~~ R A W
*raw
:PREROUTING ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A PREROUTING -m rpfilter --invert -m comment --comment BCP38 -j DROP
COMMIT
#~~~~~~~~~~~~ N A T
*nat
:PREROUTING ACCEPT [0:0]
:INPUT ACCEPT [0:0]
:POSTROUTING ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A POSTROUTING -o enp0s6.300 -j MASQUERADE
COMMIT
#~~~~~~~~~~~~ F I L T E R
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
-A INPUT -p icmp -m limit --limit 2/sec -m conntrack --ctstate NEW -j ACCEPT
-A FORWARD -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
-A FORWARD -p icmp -m limit --limit 2/sec -m conntrack --ctstate NEW -j ACCEPT
COMMIT
```

- Régles de filtrage IPv6 côté Hub : fichier `/etc/iptables/rules.v6`.

```
#~~~~~~~~~~~~ R A W
*raw
:PREROUTING ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A PREROUTING -m rpfilter --invert -m comment --comment BCP38 -j DROP
COMMIT
#~~~~~~~~~~~~ N A T
*nat
:PREROUTING ACCEPT [0:0]
:INPUT ACCEPT [0:0]
:POSTROUTING ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A POSTROUTING -o enp0s6.300 -j MASQUERADE
COMMIT
#~~~~~~~~~~~~ F I L T E R
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
-A INPUT -s fe80::/10 -j ACCEPT
-A INPUT -p ipv6-icmp -m limit --limit 2/sec -j ACCEPT
-A FORWARD -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
-A FORWARD -p ipv6-icmp -m limit --limit 2/sec -j ACCEPT
COMMIT
```

- Régles de filtrage IPv4 côté Spoke : fichier `/etc/iptables/rules.v4`.

```
#~~~~~~~~~~~~ R A W
*raw
:PREROUTING ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A PREROUTING -m rpfilter --invert -m comment --comment BCP38 -j DROP
COMMIT
#~~~~~~~~~~~~ F I L T E R
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
-A INPUT -p icmp -m limit --limit 2/sec -m conntrack --ctstate NEW -j ACCEPT
-A FORWARD -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
-A FORWARD -p icmp -m limit --limit 2/sec -m conntrack --ctstate NEW -j ACCEPT
COMMIT
```

- Régles de filtrage IPv6 côté Spoke : fichier `/etc/iptables/rules.v6`.

```
#~~~~~~~~~~~~ R A W
*raw
:PREROUTING ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A PREROUTING -m rpfilter --invert -m comment --comment BCP38 -j DROP
COMMIT
#~~~~~~~~~~~~ F I L T E R
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
-A INPUT -s fe80::/10 -j ACCEPT
-A INPUT -p ipv6-icmp -m limit --limit 2/sec -j ACCEPT
-A FORWARD -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
-A FORWARD -p ipv6-icmp -m limit --limit 2/sec -j ACCEPT
COMMIT
```

Q20. Dans les jeux de règles déjà en place, comment identifier les règles qui traitent les flux réseau dèjà enregistrés dans le suivi de communication ?

La section «7.3. États de l'espace utilisateur» du Tutoriel iptables décrit les correspondances entre les états et les flux réseau.

Q21. Quelles règles faut-il ajouter pour autoriser les nouveaux flux réseau depuis et vers l'interface de boucle locale (chaîne `INPUT`) ?

Pour que les processus locaux au système puissent communiquer entre eux, il est essentiel d'autoriser le trafic sur l'interface de boucle locale `lo`.

Q22. Quelles règles faut-il ajouter pour autoriser les nouvelles connexions SSH et les intégrer dans la table de suivi des communications ?

Le protocole de couche transport utilisé est TCP et le numéro de port utilisé par le service SSH est `2222`.

La section «7.3. États de l'espace utilisateur» du Tutoriel iptables décrit les correspondances entre les états et les flux réseau. Rechercher la clé relative aux nouveaux flux entrants.

Q23. Quelle est l'instruction qui définit la politique par défaut à appliquer sur les chaînes de la table `netfilter` ?

Il s'agit d'appliquer le principe de filtrage énoncé en début de section qui veut que tout trafic non autorisé soit interdit.

La section «9.3. Commandes» du Tutoriel iptables donne la syntaxe de configuration de cible par défaut pour les chaînes : `INPUT`, `FORWARD` et `OUTPUT`.

Une fois ces règles basiques en place, on peut aborder les filtrages réseau spécifiques à la topologie de travaux pratiques.

6. Règles de filtrage sur le routeur Hub

Dans cette section, on doit compléter les règles de filtrage pour répondre à deux objectifs :

- Le routeur Hub doit autoriser le trafic issu des routeurs Spoke vers l'Internet.
- Les demandes de connexion aux services Web hébergés sur les conteneurs desservis par les routeurs Spoke doivent être redirigées via la traduction des adresses destination.

  Voici un exemple de correspondances de numéros de ports pour l'accès aux différents services web.

Tableau 1. Correspondance entre numéro de port et service Web

numéros de port Hub : http,https	conteneur
8010,8453	`10.0.1.10` `fda0:7a62:1:0:216:3eff:feda:e1a`
8011,8454	`10.0.1.11` `fda0:7a62:1:0:216:3eff:fec4:d325`
8012,8455	`10.0.1.12` `fda0:7a62:1:0:216:3eff:fe66:86fb`
8020,8463	`10.0.2.10` `fda0:7a62:2:0:216:3eff:feda:e1a`
8021,8464	`10.0.2.11` `fda0:7a62:2:0:216:3eff:fec4:d325`
8022,8465	`10.0.2.12` `fda0:7a62:2:0:216:3eff:fe66:86fb`

Avant d'aborder les questions, on commence par afficher le contenu des deux fichiers `/etc/iptables/rules.v4` et `/etc/iptables/rules.v6` qui correspondent à la situation initiale avant de répondre aux objectifs de cette section.

- Jeu de règles pour le protocole IPv4.

```
#~~~~~~~~~~~~ R A W
*raw
:PREROUTING ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A PREROUTING -m rpfilter --invert -m comment --comment BCP38 -j DROP
COMMIT
#~~~~~~~~~~~~ N A T
*nat
:PREROUTING ACCEPT [0:0]
:INPUT ACCEPT [0:0]
:POSTROUTING ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A POSTROUTING -o enp0s6.300 -j MASQUERADE
COMMIT
#~~~~~~~~~~~~ F I L T E R
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -p icmp -m limit --limit 2/sec -m conntrack --ctstate NEW -j ACCEPT
-A FORWARD -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
-A FORWARD -p icmp -m limit --limit 2/sec -m conntrack --ctstate NEW -j ACCEPT
COMMIT
```

- Jeu de règles pour le protocole IPv6.

```
#~~~~~~~~~~~~ R A W
*raw
:PREROUTING ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A PREROUTING -m rpfilter --invert -m comment --comment BCP38 -j DROP
COMMIT
#~~~~~~~~~~~~ N A T
*nat
:PREROUTING ACCEPT [0:0]
:INPUT ACCEPT [0:0]
:POSTROUTING ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A POSTROUTING -o enp0s6.300 -j MASQUERADE
COMMIT
#~~~~~~~~~~~~ F I L T E R
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -s fe80::/10 -j ACCEPT
-A INPUT -p ipv6-icmp -m limit --limit 2/sec -j ACCEPT
-A FORWARD -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
-A FORWARD -p ipv6-icmp -m limit --limit 2/sec -j ACCEPT
COMMIT
```

Q24. Comment autoriser et enregistrer dans le mécanisme de suivi des états les flux entrants par les interfaces WAN du routeur Hub ?

Rechercher dans les pages de manuels de la commande iptables le moyen de désigner plusieurs interfaces en une seule règle.

Q25. Comment valider l'utilisation de ces deux nouvelles règles à partir d'un routeur Spoke ?

Il suffit de lancer un téléchargement depuis un routeur Spoke en utilisant successivement les protocoles IPv4 et IPv6. Ensuite, on relève les enregistrements sur le routeur Hub à l'aide de la commande conntrack.

Q26. Comment implanter les règles de traduction d'adresses IPv4 et IPv6 destination de façon à rendre accessibles les services Web configurés dans les conteneurs situés dans les réseaux desservis par les routeurs Spoke ?

Il faut rechercher la syntaxe des règles de la cible DNAT à appliquer dans la table des règles de traduction d'adresses (nat) ainsi que la syntaxe des règles à ajouter dans la chaîne `FORWARD` de la table `netfilter`.

Ces nouvelles règles doivent être conformes au tableau de correspondance donné en début de section. Bien sûr, les adresses doivent être modifiées en fonction du plan d'adressage du document Topologie Hub & Spoke avec le protocole PPPoE.

Comme pour toutes les autres sections, on n'oublie pas de sauvegarder le jeu des règles qui ont été validées.

```
$ sudo sh -c "iptables-save >/etc/iptables/rules.v4"
$ sudo sh -c "ip6tables-save >/etc/iptables/rules.v6"
```

7. Règles de filtrage sur le routeur Spoke

Comme pour la section précédente sur le routeur Hub, on doit compléter le jeu de règles de filtrage pour répondre à deux objectifs :

- Le routeur Spoke doit autoriser et enregistrer dans la table de suivi d'état les flux réseaux sortants issus du réseau des conteneurs.
- Ce même routeur Spoke doit autoriser et enregistrer dans la table de suivi d'état les flux réseaux entrants à destination des services Web hébergés par les conteneurs.

On commence par afficher le contenu des deux fichiers `/etc/iptables/rules.v4` et `/etc/iptables/rules.v6` d'un routeur Spoke qui correspondent à la situation initiale avant de traiter les questions de cette section.

- Jeu de règles pour le protocole IPv4.

```
#~~~~~~~~~~~~ R A W
*raw
:PREROUTING ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A PREROUTING -m rpfilter --invert -m comment --comment BCP38 -j DROP
COMMIT
#~~~~~~~~~~~~ F I L T E R
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -p icmp -m limit --limit 2/sec -m conntrack --ctstate NEW -j ACCEPT
-A INPUT -p tcp --syn --dport 2222 -m conntrack --ctstate NEW -m comment --comment SSH -j ACCEPT
-A FORWARD -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
-A FORWARD -p icmp -m limit --limit 2/sec -m conntrack --ctstate NEW -j ACCEPT
-A FORWARD -p tcp --syn --dport 2222 -m conntrack --ctstate NEW -m comment --comment SSH -j ACCEPT
COMMIT
```

- Jeu de règles pour le protocole IPv6.

```
#~~~~~~~~~~~~ R A W
*raw
:PREROUTING ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A PREROUTING -m rpfilter --invert -m comment --comment BCP38 -j DROP
COMMIT
#~~~~~~~~~~~~ F I L T E R
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -s fe80::/10 -j ACCEPT
-A INPUT -p ipv6-icmp -m limit --limit 2/sec -j ACCEPT
-A INPUT -p tcp --syn --dport 2222 -m conntrack --ctstate NEW -m comment --comment SSH -j ACCEPT
-A FORWARD -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
-A FORWARD -p ipv6-icmp -m limit --limit 2/sec -j ACCEPT
-A FORWARD -p tcp --syn --dport 2222 -m conntrack --ctstate NEW -m comment --comment SSH -j ACCEPT
COMMIT
```

Q27. Comment autoriser et enregistrer dans le mécanisme de suivi des états les flux sortants par l'interface WAN du routeur Spoke ?

Rechercher dans les pages de manuels de la commande iptables le moyen de désigner une interface ainsi que le sens des flux qui transitent par cette interface.

Q28. Comment valider l'utilisation de ces deux nouvelles règles à partir d'un routeur Spoke ?

Il suffit de lancer un téléchargement depuis un conteneur desservi par le routeur Spoke en utilisant successivement les protocoles IPv4 et IPv6. Ensuite, on relève les enregistrements sur le même routeur Spoke à l'aide de la commande conntrack.

Q29. Comment autoriser les flux Web entrants par l'interface WAN vers les conteneurs ?

Rechercher dans les options de la commande iptables celles qui permettent de désigner les interfaces d'entrée et de sortie ainsi que les numéros de ports associés au service Web.

Q30. Comment valider l'utilisation des deux règles ajoutées dans la question précédente ?

Reprendre, depuis le routeur Hub, l'utilsation de la commande wget telle qu'elle a été présentée dans la section Routeurs Spoke du support Topologie Hub & Spoke avec le protocole PPPoE.

8. Documents de référence

IETF & IANA

Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing, BCP 38, `rp_filter`

Le document standard RFC2827 Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing est un guide de bonne pratiques pour se protéger contre l'usurpation des adresses sources. Dans le monde GNU/Linux, la fonction clé est appélée `rp_filter` pour Reverse Path Filtering.

Distribution Debian GNU/Linux

Manuel de référence Debian

Manuel de référence Debian : configuration du réseau : chapitre du manuel de référence Debian consacré à la configuration réseau.

Site inetdoc.net

Configuration d'une interface de réseau local

Configuration d'une interface de réseau local : identification du type d'interface, de ses caractéristiques et manipulations des paramètres. Ce support fournit une méthodologie de dépannage simple d'une connexion réseau.

Fonctions réseau du noyau Linux

Configuration des fonctions réseau & compilation du noyau Linux : présentation et configuration des fonctions réseau du noyau LINUX

Didacticiel sur Iptables

Tutoriel iptables : guide très complet sur le fonctionnement du filtrage réseau avec les noyaux Linux.

Guide Pratique du NAT

Guide Pratique du NAT : Ce document décrit comment réaliser du camouflage d'adresse IP, un serveur mandataire transparent, de la redirection de ports ou d'autres formes de Traduction d'adresse réseau (Network Address Translation ou NAT) avec le noyau Linux 2.4.