Création le : 23/03/2017
Quentin Giorgi.

TP – Implémentation d'une architecture d'accès à Internet

Préparation et recommandations

Une entreprise utilise le plus souvent un plan d'adressage privé pour l'ensemble des équipements internes à son réseau. Cela pose un problème lors de l'accès à Internet, notamment lorsque les utilisateurs utilisent leur browser, puisque ces adresses sont non routables. Pour corriger cela il existe plusieurs solutions comme nous allons le voir dans le reste du TP.

Pré-requis :
Connaitre les définitions des termes Firewall, DMZ.
Connaitre les commandes UNIX suivantes : ip addr , ip route, ping, traceroute, tcpdump.

Travail à effectuer :

Lire l'intoduction de la documentation sur le firewall linux :

https://wiki.nftables.org/

Introduction

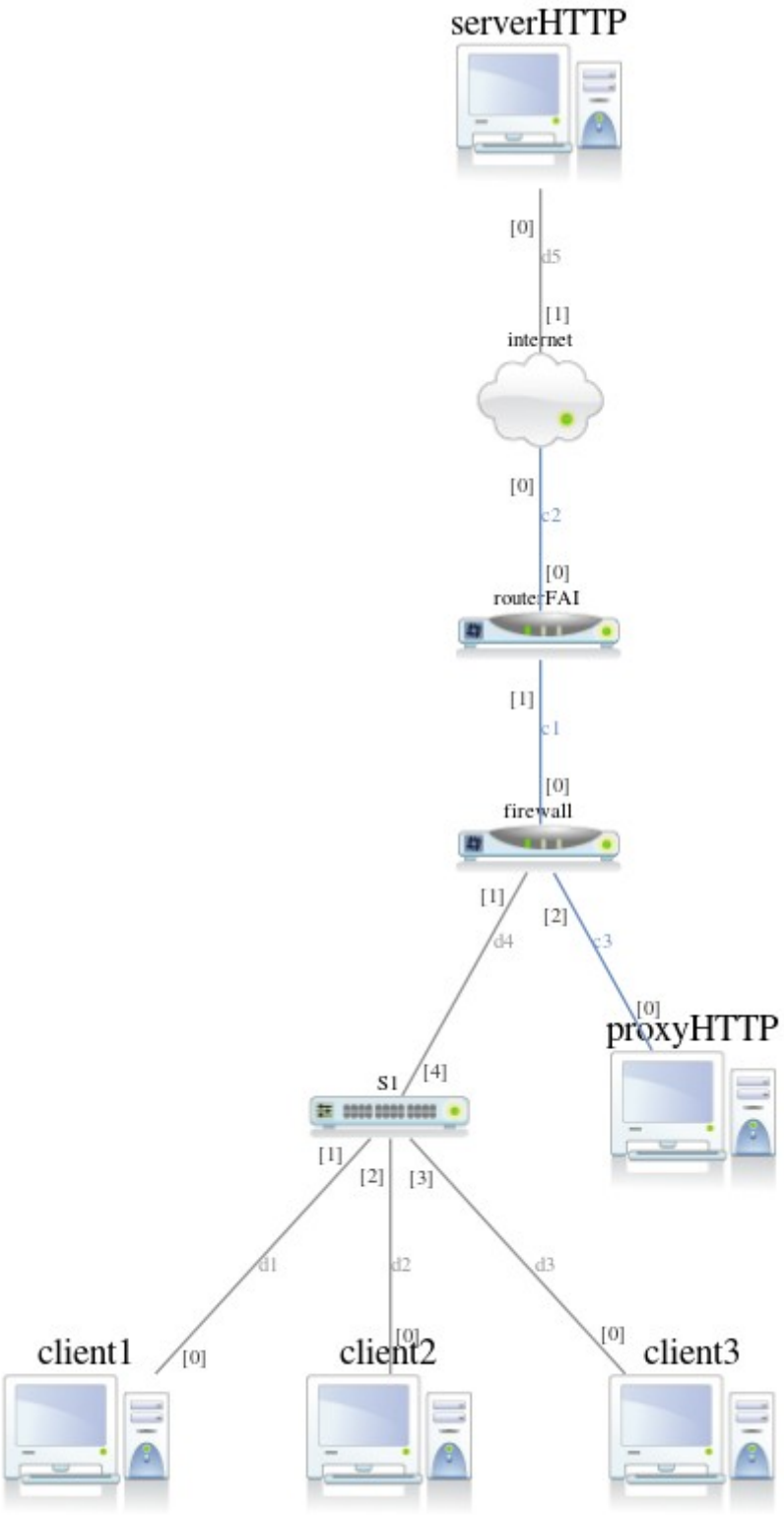
Vous êtes en charge de réaliser l'accès à Internet d'une petite entreprise, pour simuler cette architecture, vous utiliserez un projet comme représenté en figure 1.

Les usagers internes sont appelés « clients »

Pour cela vous pouvez administrer les équipements client1,client2,client3, switch, firewall et proxy, représentant les équipements locaux, utilisant des adresses IP privées. Le proxy est en DMZ (192.168.110.1/24), les « clients » dans le réseau interne (192.168.100.0/24) en .1 .2 et .3 respectivement pour client1 client2 et client3.
Toutes les interfaces du firewall ont l'adresse IP 254 pour la partie station (192.168.100.254, 192.168.110.254, 193.23.23.254)

Vous avez un contrat avec un fournisseur d'accès Internet représenté par le routeur R1, et Internet représenté par N1 et serveurs_web. **Bien sûr vous n'avez pas d'accès de configuration à ces équipements.** Votre fournisseur d'accès Internet vous fourni le routeur R1 configuré ainsi qu'une plage d'adresses IP publiques 193.23.23.0/24 librement utilisable pour vous (sauf l'adresse .1 utilisée par le routeur) [NOTE : Vous pouvez être satisfaits car actuellement il est presque impossible d'obtenir ce genre d'adresses:)]

Lancez marionnet, chargez le projet TP2-NE372.mar et lancez tous les éléments via le bouton « Start All »



Solution 1 : Routage, NAT et filtrage des flux.

Avec cette solution les clients accèdent directement aux serveurs Internet sans passer par un proxy HTTP, les clients ayant des adresses privées, une translation d'adresse doit être effectuée pour que ces clients puissent accèder à Internet. Cette communication doit fonctionner pour tout type de flux. (ici nous nous limiterons à autoriser les seuls flux sortants HTTP et ICMP)

Pour créer ce genre d'architecture, il faut une démarche structurée, définir des étapes et valider chaque étape avant de passer à la suivante. Pour cette architecture simple, les trois étape sont le routage, le NAT puis le filtrage.

1 - Routage.

- Activer le routage sur le firewall, et faites en sorte que cette modification soit effectuée à chaque reboot en modifiant le fichier /etc/sysctl.conf

- Indiquer la route par défaut pour les clients, pour le firewall et le proxy et installez les sur les clients (soit via l'interface marionnet soit sur le terminal avec la commande ip route dont vous regarderez le manuel).

Question : Sans translation d'adresse, quelles sont les différentes stations qui peuvent communiquer entre-elles ? Faites des tests de ping entre ces stations afin de vérifier que le routage fonctionne à travers le firewall. Est-ce conforme à l'attendu ?

2 – Translation d'adresse.

- Le client 1 va être translaté vers internet en utilisant l'adresse IP publique du firewall (on appelle cela du masquerading), effectuez cette translation d'adresse en appliquant la règle appropriée sur le firewall :

-le client2 doit être différencié vis à vis des serveurs web et sa translation d'adresse utilisera donc l'adresse source 193.23.23.2, effectuez cette translation d'adresse, que faut-il faire de plus pour que cela fonctionne ?

Question : vérifiez en effectuant un ping depuis client1, client2, client3, vers www.monsite.fr et www.mysite.com, et observez sur le firewall la translation d'adresse en utilisant la commande ***tcpdump -i eth0 -n*** puis ***tcpdump -i eth1 -n***

Question : Avec quelle adresse source les paquets icmp arrivent-ils sur le serveur web ? Vérifiez avec tcpdump.

3 – Filtrage.

Maintenant que le routage et la translation d'adresse fonctionne, vous allez filtrer les accès des clients vers Internet pour n'autoriser que les flux conformément à la table ci-dessous.
[NOTE : Jusqu'à présent on ne s'est pas posé la question des résolutions de noms DNS, car le proxy est aussi un serveur cache DNS pour l'infrastructure client.]

Source	Destination	Protocoles	Action
Client1	Exterieur	HTTP,HTTPS	Autoriser
Client2	Exterieur	HTTP,HTTPS	Autoriser
Tous	Tous	ICMP	Autoriser
Proxy	Exterieur	DNS	Autoriser
Tous les clients	proxy	DNS	Autoriser

Quand on met en place un firewall, il faut la aussi une démarche structurée :
On commence par créer une table de filtrage
nft add table ip filter

Puis par créer une « chain » de politique par défaut « tout interdire » :
nft 'add chain ip filter forward { type filter hook forward priority 0 ; policy drop ; }';

Puis par autoriser dans cette « chain » les connexions établies :
nft insert rule ip filter goout ct state established counter accept

Ensuite on ajoute les règles de filtrage…

nft add rule ip filter forward ….

Question: Essayez d'accéder au port 80 de www.monfakesite.fr, que constatez-vous ? Que pouvez vous dire sur le niveau OSI auquel se place le filtrage effectué ainsi ?

Solution 2 : filtrage applicatif par proxy HTTP.

Avec cette solution les clients n'accèdent plus directement aux serveurs web Internet mais doivent passer par un proxy HTTP, qui est le seul à pouvoir acceder à Internet sur les ports 80 et 443. Cette solution permet à l'entreprise de filtrer de manière plus fine les différents accès des clients aux serveurs web, notamment vérification protocolaire, autorisations d'accès, mise en cache des données téléchargées pour éviter de consommer de la bande passante, etc.

Le proxy ayant une adresse privée, une translation d'adresse doit être effectuée pour qu'il puisse accèder à Internet. Seul client3 utilisera cette solution.

Pour cette architecture un peu plus complexe, les étapes sont le routage, le NAT, le filtrage et la mise au point des services (proxy HTTP). Procédez comme vous venez d'apprendre, par étape.

A l'aide des questions suivantes effectuer, et valider les étapes routage et NAT.

Question : doit-il y avoir une translation d'adresse pour client3 ?
Question : Quelle doit être la route par défaut de client3 ?

Question : Le proxy doit accèder à Internet, sa translation d'adresse utilisera donc l'adresse source 193.23.23.3, effectuez cette translation d'adresse sur le firewall et vérifiez qu'il peut acceder à www.monsite.fr et www.mysite.com.

Question : Faites un tableau comme précédemment en indiquant les nouveaux flux nécessaires à autoriser. Pour cela répondez d'abord aux questions suivantes ?

Question : Le client3 a t-il besoin d'un resolver DNS ? Le flux DNS doit-il être autorisé pour client3 ?

Question : Sur quel port tcp ecoute le proxy HTTP ? Quel est le fichier de configuration de ce proxy ?

Configuration du service pour les clients

- Faites en sorte que client3 passe par le proxy pour les requêtes HTTP via la commande wget, et vérifiez que vous accèdez à Internet via le proxy. Pour cela vous pouvez regarder les logs sur le proxy dans /var/log/tinyproxy/tinyproxy.log