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 :

Connaître les définitions des termes Firewall, DMZ.
Connaître les commandes UNIX suivantes : ip addr, ip route, ping, traceroute, tcpdump.

Travail à effectuer :

Lire de la documentation sur le firewall linux :
https://wiki.nftables.org/

https://bind9.readthedocs.io/en/v9_16_10/

Introduction

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

Pour cela, vous pouvez administrer les équipements client1, client2 (les usagers internes sont appelés « clients »), R1, srvDNS, srvHTTP, R2_home, R4_office, proxy.

Vous avez un contrat avec un fournisseur d'accès Internet représenté par le routeur R3_fai, et Internet représenté par N1. Bien sûr, vous n'avez pas d'accès de configuration à ces équipements. Votre fournisseur d'accès Internet vous fournit le routeur R3_fai déjà configuré.

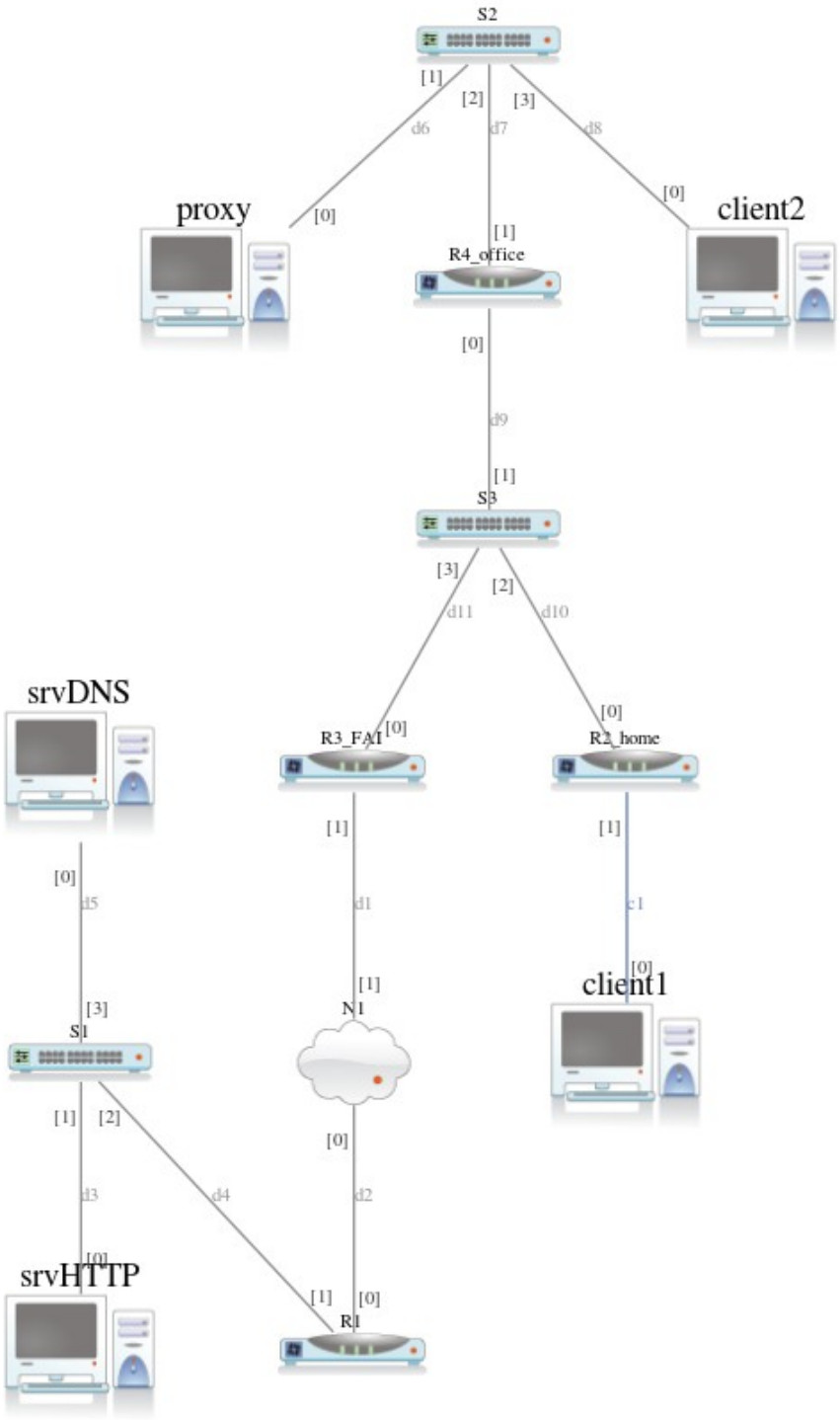
S2
[1]
[2]
[3]
d6
d7
d8
proxy
[0]
[1]
R4_office
[0]
client2
[0]
d9
[1]
S3
[3]
[2]
d11
d10
srvDNS
R3_FAI
[0]
[0]
R2_home
[1]
[1]
[0]
d5
d1
c1
[1]
N1
client1
[0]
[3]
S1
[1]
[2]
[0]
d3
d4
d2
[0]
srvHTTP
[1]
[0]
R1

Figure 1

Mise en œuvre de la solution pour le client1

Le client1 doit pouvoir accès à Internet en utilisant l'adresse IP publique de sa passerelle par défaut.

Configurer le routeur **R2_home** pour cela.

Vous pouvez le vérifier en effectuant des requêtes ICMP sur l'adresse 193.23.23.2.

Configurer le routeur R2_home pour que seuls les protocoles HTTP et DNS puissent sortir vers Internet ainsi que les sessions déjà établies.

Question : Quelles sont les commandes utilisées pour la configuration du filtrage ?

Configuration du serveur DNS

Il vous faudra créer la zone titi.fr sur le serveur **srvDNS** avec un enregistrement A qui pointe sur l'adresse publique du routeur **R1**

Configurer les clients pour qu'ils utilisent le serveur **srvDNS** comme résolveur DNS

Question : Quelle adresse IP utilisez-vous ? Est-ce que ça fonctionne en l'état ?

Mise en œuvre de la solution pour l'accès aux serveurs

Démarrer le serveur HTTP sur srvHTTP avec la commande : `systemctl enable --now lighttpd`

Les serveurs DNS et web doivent être accessibles depuis le client en utilisant l'IP du routeur **R1** (193.23.23.2).

Pour cela il va falloir configurer de la redirection de ports.

Il faudra donc rediriger les ports liés au protocole DNS sur le serveur **srvDNS** et ceux liés à HTTP sur le serveur **srvHTTP**.

Question : Quels sont les ports à rediriger ?

Question : Quelle commande utilisez-vous ?

Ensuite, configurez le client pour qu'il utilise comme résolveur le serveur **srvDNS**.

À l'aide des commandes `dig` & `curl`, vérifiez que l'ensemble fonctionne correctement.

Grâce aux commandes `tcpdump` & `conntrack -L`, étudiez le fonctionnement du suivi des connexions avec les protocoles TCP et UDP.

Question : Quelle conclusion pouvez-vous tirer sur le fonctionnement de conntrack ?

Mise en œuvre de la solution pour le client2

Le client2 doit avoir accès à internet en utilisant un serveur proxy HTTP (tinyproxy).

Question : Doit-il y avoir une translation d'adresse pour client2 ?

Question : Quelle doit être la route par défaut de client2 ?

Le proxy doit accéder à Internet, sa translation d'adresse utilisera l'adresse publique du routeur. Effectuez cette translation d'adresse sur le routeur **R4_office** et vérifiez qu'il peut accéder à titi.fr.

Question : Faites un tableau en indiquant les flux nécessaires à autoriser.

Pour cela, répondez d'abord aux questions suivantes **:**

→**Question : Le client2 a-t-il besoin d'un résolveur DNS dans le cadre de l'utilisation d'un serveur proxy ? Le flux DNS doit-il être autorisé pour client2 ?**

→**Question : Sur quel port TCP écoute le proxy HTTP ? Quel est le fichier de configuration de ce proxy ?**

Configuration du service pour les clients

- Faites en sorte que client2 passe par le proxy pour les requêtes HTTP via la commande wget, et vérifiez que vous accédez à Internet à travers le proxy. Pour cela vous pouvez regarder les logs sur le proxy dans /var/log/tinyproxy/tinyproxy.log

Question : Quels sont les avantages et inconvénients de cette solution ?