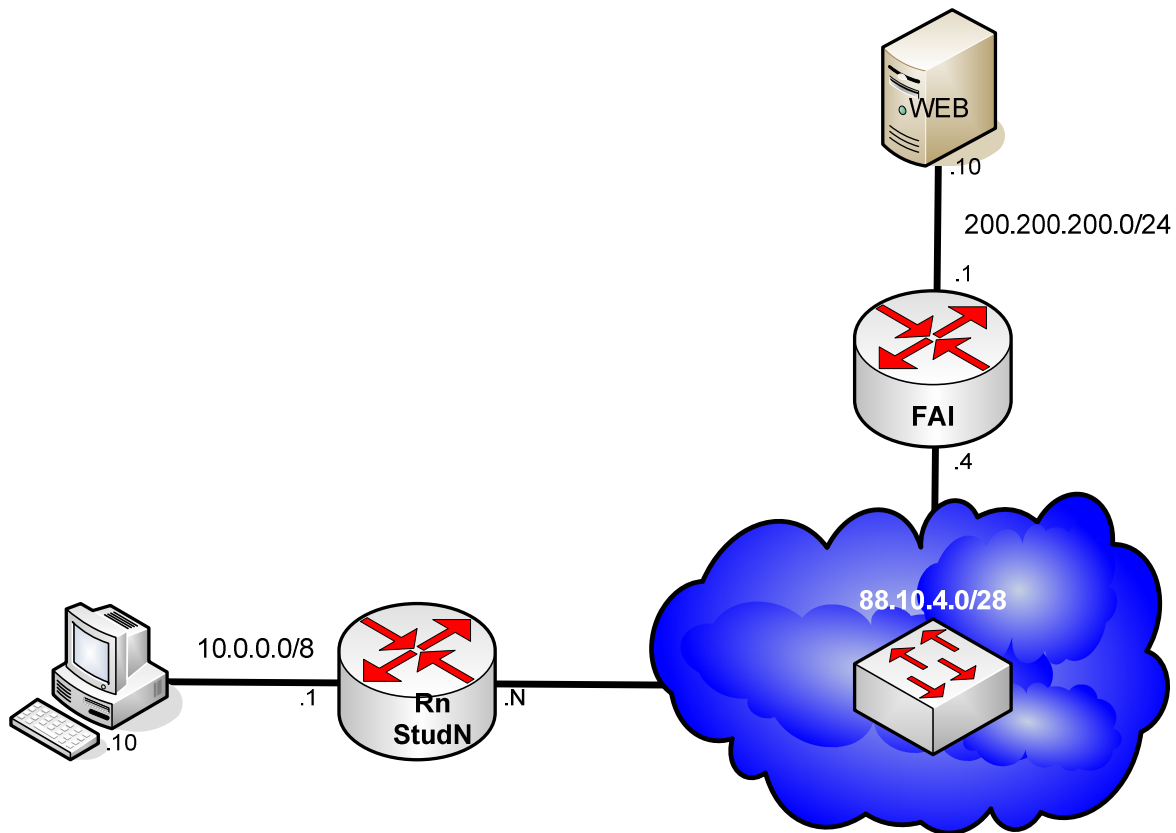


TP PAT

1. Topologie de travail

La topologie de travail pour un étudiant N (N compris entre 1 et 3) sera la suivante :



avec pour l'étudiant N :

Nom	Adresse
Fa0/0 de GW StudN	10.0.0.1/8
PC	10.0.0.10/8
Fa0/1 de GW StudN	88.10.4.N/28

Le routeur FAI étant un routeur commun ayant comme adresses :

- 88.10.4.4 pour l'interface fa0/0 ;
- 200.200.200.1/24 pour l'interface fa0/1 ;

2. Configuration du routeur

Du grand classique : accès telnet (mot de passe), accès console (synchronisation de l'affichage, mot de passe, temps d'attente), mot de passe administrateur, désactivation de la recherche DNS, interfaces.

Au moyen de la commande `ip dhcp pool`, mettez en place un serveur DHCP distribuant les adresses du réseau local. Attention toutefois au fait que votre PC devra toujours recevoir l'adresse 10.0.0.10.

En passant votre PC en demande d'adresse automatique, vérifiez que ce serveur fonctionne

Au niveau du routage, vous placerez une route statique par défaut, le saut suivant étant l'adresse 88.10.4.4.

2. Mise en place de la traduction dynamique d'adresses avec surcharge de port

Vous allez mettre en place une traduction dynamique des adresses avec surcharge de port pour le réseau 10.0.0.0/8. Pour cela, vous devrez :

1. spécifier l'interface de votre routeur connectée à la zone `inside`, et celle connectée à la zone `outside` ;
2. indiquer au moyen d'une ACL le trafic qui sera traduit ;
3. écrire la règle de traduction (commande `ip nat inside source list`).

Une fois cette configuration réalisée, effectuez un ping de votre PC vers le serveur WEB.

Est-ce que cela a fonctionné ?

Si non, vous avez un problème et revenez au début du TP !

Si oui, expliquez pourquoi il n'a pas été nécessaire de mettre une route statique sur FAI ?

Sur votre routeur, au moyen de la commande `clear ip nat translation *`, nettoyez la table de traduction, puis lancez une capture de trames sur votre PC et sur le PC WEB. Depuis votre PC, effectuez alors une requête HTTP sur le PC WEB (n'oubliez pas de lancer mini-zazou). Une fois la page chargée :

Complétez au moyen de la commande `sh ip nat translation` le tableau suivant :

Pro	Inside global	Inside local	Outside local	Outside global

et retrouvez ces informations sur les captures de trames.

Depuis le serveur WEB, est-il possible de faire un ping sur l'adresse Inside local ?

Depuis le serveur WEB, est-il possible de faire un ping sur l'adresse Inside global ?

Complétez le texte suivant :

Lors d'une traduction dynamique d'adresses avec surcharge de port, pour un paquet voyageant de la zone vers la zone, l'adresse privée du paquet est remplacée par l'adresse de l'interface de du routeur.

Pour le trafic retour en provenance de la zone et à destination de la zone, l'adresse publique du paquet est remplacée par l'adresse qui était à l'origine du trafic.

Depuis la zone, il est impossible d'envoyer un trafic dans la zone si le trafic en question ne correspond pas au retour d'un trafic préalablement initié depuis la zone.....

3. ICMP

La traduction dynamique de port que vous avez mise en place fonctionne logiquement avec de nombreux protocoles sous TCP ou UDP, mais fonctionne également avec ICMP ce qui est

beaucoup plus étonnant quand on se rappelle que la notion de port n'existe pas avec ce protocole. Lancer donc une capture de trames sur votre PC, puis faites un ping de votre PC vers le serveur. Une fois ceci fait, arrêtez la capture, observez sur le routeur la table des traductions.

Quel est le nom du champ dans le PDU ICMP permettant au routeur de réaliser sa traduction d'adresse avec surcharge de port ?

4. Mise en place de la traduction statique de port

Vous allez maintenant faire en sorte d'externaliser le port 80 en tcp de votre PC sur l'adresse 88.10.4.1N/28 port 8080 (utilisez pour cela la commande `ip nat inside source static tcp`).

Depuis le serveur WEB, est-il possible de faire une requête HTTP sur l'adresse Inside global port 8080 (n'oubliez pas de lancer mini-zazou sur votre machine) ?

Lancez wireshark sur votre PC, puis faites un ping sur l'adresse 88.10.4.1N/28 depuis le serveur WEB.

Dans la capture sur votre PC, recevez-vous des message `echo-request` ?
Depuis le serveur WEB avez-vous eu un `echo-reply` indiquant un succès ? ¹

5. Mise en place d'une ACL

Sur votre routeur, mettez en place une ACL autorisant uniquement le trafic attendu pour les protocoles `icmp` et `http` à pénétrer sur votre routeur.

Faites tester votre ACL par le chargé de TP.

Depuis votre PC, est-il toujours possible de faire une requête HTTP sur PC WEB ?
Depuis votre PC, est-il toujours possible de faire un ping sur le serveur WEB ?

Depuis votre PC, si vous faites un ping sur l'adresse 8.8.8.8, recevez-vous le message "destination inaccessible" ?

Pourquoi n'en recevez-vous pas ?

Corrigez cette erreur en rajoutant une règle à votre ACL (indication il faut laisser revenir les message `icmp` de type `host-unreachable`)

Depuis le serveur WEB, est-il encore possible de faire une requête HTTP sur l'adresse Inside global ?

¹ Et oui, car vous êtes la victime d'un bug (ici c'est le routeur qui vous répond) alors que votre machine est bien invisible depuis l'extérieur