nat et pat

Table des matières

[Introduction : 2](#_Toc190019523)

[Présentation NAT et PAT : 2](#_Toc190019524)

[1: NAT statique : 2](#_Toc190019525)

[2: NAT dynamique : 3](#_Toc190019526)

[3: PAT : 3](#_Toc190019527)

[Exercice 1 : 4](#_Toc190019528)

[4: Observer la fonction NAT : 4](#_Toc190019529)

[Envoi d’une requête HTTP à un serveur web externe depuis un hôte interne : 4](#_Toc190019530)

[Envoi d’une requête HTTP à un serveur web interne depuis un hôte externe : 9](#_Toc190019531)

[Exercice 3 : NAT statique : 9](#_Toc190019532)

[5: Configuration : 9](#_Toc190019533)

[6: Fonctionnement : 10](#_Toc190019534)

[Exercice 4 : NAT dynamique partie 1 11](#_Toc190019535)

[Exercice 5 : NAT dynamique partie 2 : 12](#_Toc190019536)

[7: Configuration du rip : 12](#_Toc190019537)

[8: Configuration du nat : 13](#_Toc190019538)

[Exercice 7 : NAT : redirection de ports : 14](#_Toc190019539)

[9: FTP : 16](#_Toc190019540)

[10: Ajout de mon site web : 18](#_Toc190019541)

[Exercice n°7 : Nat dynamique IPv6 en IPv4 – NAT PT 20](#_Toc190019542)

[Modification de notre réseau : 24](#_Toc190019543)

[11: Création des différents réseaux : 24](#_Toc190019544)

[Les nouvelles adresses IP : 25](#_Toc190019545)

[Modification des noms/adresses IP : 25](#_Toc190019546)

[12: Routage : 26](#_Toc190019547)

[13: Serveur DNS, DHCP et AAA : 26](#_Toc190019548)

[DNS : 26](#_Toc190019549)

[DHCP : 27](#_Toc190019550)

[AAA : 29](#_Toc190019551)

[14: Serveur FTP : 30](#_Toc190019552)

[15: Serveur Messagerie : 31](#_Toc190019553)

[Configuration : 32](#_Toc190019554)

[Test : 33](#_Toc190019555)

[16: Serveur TFTP : 33](#_Toc190019556)

[17: Serveur log : 35](#_Toc190019557)

[18: Routeur WRT300N : 36](#_Toc190019558)

[19: Mise en place du NAT/PAT : 37](#_Toc190019559)

[20: Points forts du réseau : 38](#_Toc190019560)

[21: Points faibles du réseau : 39](#_Toc190019561)

[Conclusion : 39](#_Toc190019562)

[Sources : 40](#_Toc190019563)

**Dans ce TP, tous les carrés gris sont des paramètres à changer selon le routeur ou les adresses IP valides. J’ai fait ça pour éviter de mettre des captures d’écran qui se répètent**

# Introduction :

Dans ce TP, nous explorons la configuration et le fonctionnement du Network Address Translation (NAT) et de la redirection des ports, des mécanismes essentiels pour permettre aux réseaux privés de communiquer avec l’extérieur tout en optimisant l’utilisation des adresses IP publiques. Le NAT est une technologie largement utilisée pour masquer les adresses privées des équipements internes et leur permettre d’accéder à Internet en toute sécurité. Parmi les différentes formes de NAT, nous nous concentrerons ici sur le NAT statique, dynamique et le Port Address Translation (PAT).

L’un des aspects clés de ce TP est la redirection des ports, qui permet de rendre accessible un service interne (tel qu’un serveur web ou FTP) depuis l’extérieur via une adresse IP publique. Cette technique est essentielle dans un contexte professionnel où certaines applications doivent être accessibles aux clients et partenaires tout en restant hébergées dans une infrastructure sécurisée.

À travers divers exercices pratiques, nous allons configurer et tester le NAT statique et dynamique, observer les traductions d’adresses en action, et vérifier le bon fonctionnement de la redirection de ports pour assurer l’accessibilité des services internes. Ce TP nous permettra de maîtriser l’implémentation du NAT, de comprendre son rôle dans la sécurité et la connectivité d’un réseau, et de simuler des scénarios réels d’entreprise où l’accès aux services internes depuis Internet doit être contrôlé et sécurisé.

# Présentation NAT et PAT :

## NAT statique :

Le NAT statique est un mécanisme de traduction d’adresses qui associe une adresse IP publique unique à une adresse IP privée fixe. Ce type de NAT est principalement utilisé pour rendre des appareils ou services internes accessibles depuis l’extérieur, comme un serveur web ou FTP. Avec le NAT statique, une correspondance permanente est créée entre une adresse privée et une adresse publique. Par exemple, une adresse IP publique spécifique peut être mappée à un serveur interne pour que celui-ci soit accessible depuis Internet tout en maintenant l’isolation des autres machines internes. Cependant, ce type de NAT ne résout pas la pénurie d’adresses IPv4, car chaque adresse publique est utilisée pour une seule machine privée.Une image contenant texte, capture d’écran, Police, conception

Description générée automatiquement

## NAT dynamique :

Le NAT dynamique est une méthode qui permet d’attribuer dynamiquement une adresse publique à une machine interne à partir d’un pool d’adresses IP publiques disponibles. Contrairement au NAT statique, l’association entre une adresse privée et une adresse publique n’est pas fixe : une machine privée utilise temporairement une adresse publique du pool pour sa communication, et cette adresse est libérée lorsqu’elle n’est plus nécessaire. Ce type de NAT est utile dans les environnements où plusieurs appareils doivent accéder à Internet, mais où un nombre limité d’adresses publiques est disponible. Il permet ainsi de partager efficacement les ressources IP tout en garantissant une certaine flexibilité.Une image contenant texte, capture d’écran, Police, conception

Description générée automatiquement

## PAT :

Le PAT (Port Address Translation), aussi appelé NAT Overload, est une variante du NAT dynamique. Avec le PAT, plusieurs appareils internes peuvent partager une seule adresse IP publique. Pour différencier les connexions provenant des différentes machines internes, le PAT utilise les numéros de ports associés aux sessions. Par exemple, si deux appareils internes accèdent simultanément à Internet en utilisant la même adresse publique, le routeur NAT ajoute des informations sur les ports sources pour identifier chaque session. Le PAT est la méthode la plus couramment utilisée, car elle permet à un grand nombre de machines d’accéder à Internet en utilisant une seule adresse publique, ce qui est particulièrement efficace pour les réseaux avec des ressources IP limitées.Une image contenant texte, capture d’écran, conception

Description générée automatiquement

# Exercice 1 :

## Observer la fonction NAT :

### Envoi d’une requête HTTP à un serveur web externe depuis un hôte interne :

a)

Une image contenant texte, Appareils électroniques, capture d’écran, Police

Description générée automatiquement

Lors d’une requête DNS, dans l’enveloppe ARP, le poste cherche une adresse mac pour l’adresse IP 192.168.1.20 comme marqué dans la destination IP (Dest. IP).

b)

Une image contenant texte, Appareils électroniques, capture d’écran, Police

Description générée automatiquement

Le périphérique qui répond à la requête ARP émise par Customer PC est [www.customerserver.com](http://www.customerserver.com), correspondant à l’adresse IP 192.168.1.10. L’adresse MAC fournie par [www.customerserver.com](http://www.customerserver.com) est 00E0.B073.922C. Cette adresse MAC est utilisée pour permettre à Customer PC de communiquer directement avec le serveur en identifiant sa destination sur le réseau local.

c) Le nouveau protocole qui apparait est le DNS (Domain Name System) :

Une image contenant texte, capture d’écran, ligne, Police

Description générée automatiquement

Le protocole DNS associe un nom de domaine à une adresse IP.

Cette requête vise à résoudre le nom de domaine www.ipserver.com en une adresse IP. Le port source utilisé est 1025, tandis que le port de destination est 53, dédié aux communications DNS. Le champ "Transaction ID: 0x72fa" permet de suivre cette requête et de l'associer à la réponse correspondante. Cette configuration pour initie une résolution de nom de domaine.

Une image contenant texte, reçu, capture d’écran, nombre

Description générée automatiquementDans cette capture, on observe les détails d’un paquet DNS sortant généré par le client. Voici une analyse des couches affichées :

Ethernet II : Cette couche montre l’adresse MAC source (00:E0:B073.922C) et l’adresse MAC de destination (00:E0:B0EA:BDA8) qui sont nécessaires pour la transmission locale dans le réseau.

IP : L’adresse IP source est 192.168.1.10 et la destination est 192.168.1.20. Cela indique un échange entre deux machines locales.

UDP : Le port source est 1025 et le port destination est 53, ce qui est typique pour une requête DNS, car le port 53 est utilisé pour les résolutions DNS.

DNS Header et Query : Le paquet contient une requête DNS pour résoudre le nom de domaine www.ispserver.com. Cela permet au client d’obtenir l’adresse IP correspondante pour initier une connexion.

d)

Une image contenant texte, capture d’écran, nombre, Police

Description générée automatiquement

L’adresse IP du serveur www.customerserver.com est 192.168.1.10

e)

Une image contenant texte, capture d’écran, nombre, affichage

Description générée automatiquement

Customer PC doit résoudre l’adresse MAC de serveur [www.ipserver.com](http://www.ipserver.com) après la résolution DNS. Il a eu celle de [www.customerserver.com](http://www.customerserver.com) et pas celle qu’il veut.

f)

Une image contenant texte, capture d’écran, Police, nombre

Description générée automatiquement

La requête HTTP est envoyée une fois que l’adresse IP du serveur est connue (209.165.202.131) et que l’adresse MAC de la passerelle est résolue (0030.A38A.4701).

g)

Une image contenant texte, Appareils électroniques, capture d’écran, Police

Description générée automatiquement

Le routeur utilise un mécanisme de translation dynamique (NAT/PAT) pour permettre la communication entre le réseau privé et Internet. Lorsqu'un paquet entre dans le routeur (inbound), l'adresse source est 192.168.1.10 (adresse privée du PC) et la destination est 209.165.202.131 (adresse du serveur du FAI). En sortie du routeur (outbound), l'adresse source privée est remplacée par une adresse publique traduite, 209.165.201.2 pour de rendre le paquet routable sur Internet tandis que l'adresse de destination reste inchangée. Ce processus est géré par le routeur qui enregistre l'entrée correspondante dans sa table NAT. Cette entrée permet d'associer la réponse entrante à l'adresse privée d'origine, ce qui garantit une communication fluide entre le réseau local et les serveurs distants.

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

k)

Lorsque la réponse HTTP du serveur FAI (209.165.202.131) arrive au routeur client, une traduction du NAT est faite pour rediriger le paquet vers le PC interne. Initialement, le paquet entrant (inbound) a pour source 209.165.202.131 (serveur FAI) et pour destination 209.165.201.2 (adresse publique traduite, Inside Global). Le routeur consulte alors sa table NAT dynamique où il trouve une correspondance entre l'adresse publique (209.165.201.2) et l'adresse privée locale correspondante (192.168.1.10, Inside Local). Grâce à cette correspondance, le routeur remplace l'adresse de destination publique par l'adresse privée du PC (192.168.1.10), tout en conservant l'adresse source d'origine (209.165.202.131). Ainsi, le paquet modifié est routé vers le réseau interne (outbound).

### Envoi d’une requête HTTP à un serveur web interne depuis un hôte externe :

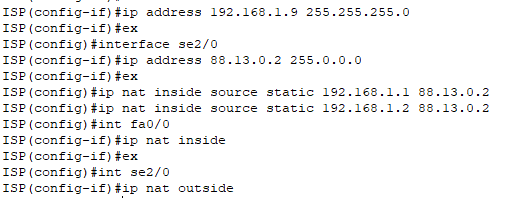
Une image contenant texte, capture d’écran, Police, nombre

Description générée automatiquement

Dans cette capture, le routeur utilise un mécanisme de translation dynamique (NAT/PAT) pour gérer le trafic entre les réseaux. Le paquet entrant (inbound) provient de l'adresse source 209.165.202.130 (dispositif du réseau de l'ISP) et a pour destination 209.165.201.5 (adresse publique traduite représentant le client). En sortie (outbound), l'adresse source 209.165.202.130 reste inchangée, mais le routage s'effectue à travers un port série (Serial0/0/0), comme indiqué dans la couche 1 (HDLC Frame). Ce mécanisme NAT permet au routeur de diriger les paquets de manière appropriée en s'appuyant sur sa table NAT, où sont enregistrées les correspondances entre les adresses publiques traduites et les adresses internes du réseau local, ce qui garantit une communication fluide entre les dispositifs internes et les serveurs externes.

# Exercice 3 : NAT statique :

## Configuration :



Je mets en place une translation d'adresses statique (Static NAT) pour permettre à des appareils du réseau interne d'être accessibles depuis l'extérieur avec des adresses publiques spécifiques. Tout d'abord, l'adresse IP 192.168.1.9 est configurée sur l'interface interne fa0/0 avec un masque correspondant à un sous-réseau privé. Ensuite, l'interface externe se2/0 est configurée avec l'adresse publique 88.13.0.2 qui servira de point de contact sur Internet.

Les commandes ip nat inside source static permettent d'associer les adresses privées internes 192.168.1.1 et 192.168.1.2 à l'adresse publique 88.13.0.2. Cela signifie que tout trafic entrant à destination de 88.13.0.2 sera redirigé vers ces adresses internes.

Les interfaces fa0/0 est à l'intérieur (ip nat inside) et se2/0 à l’exterieur (ip nat outside) du réseau NAT.

## Fonctionnement :

Une image contenant texte, capture d’écran, Police, algèbre

Description générée automatiquement

La commande show ip nat statistics indique qu'une seule traduction est active, comprenant 2 entrées statiques. L'interface interne est FastEthernet0/0, tandis que l'interface externe est Serial2/0. Aucun paquet n'a encore été traduit (Hits: 0, Misses: 0) car je viens de la configurer.

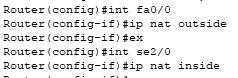
Une image contenant texte, capture d’écran, Police, ligne

Description générée automatiquement

La commande show ip nat translation fournit une correspondance détaillée entre l'adresse publique (Inside Global) 88.13.0.2 et l'adresse privée interne (Inside Local) 192.168.1.2. Ce qui reflète une configuration NAT statique où une adresse publique unique est mappée à une machine spécifique dans le réseau privé. Les colonnes Outside Local et Outside Global sont vides ici, car aucune requête spécifique depuis une source externe n'a encore été enregistrée. Cette configuration garantit que les paquets entrants destinés à 88.13.0.2 sont acheminés correctement vers la machine interne associée.

Pour mesurer les flux réseaux je regarderai Outside local et Outside Global pour voir les les requêtes entrantes et sortantes NAT et Hits (le nombre de paquets pour lesquels une correspondance valide a été trouvée dans la table NAT) et Misses (compte les paquets pour lesquels aucune correspondance n'a été trouvée dans la table NAT) pour voir les paquets traduits.

Les paquets ICMP restent bloqué entre les deux routeurs car j’ai mal configuré les interfaces de sortie et d’entrer sur le router0. L’interface fa0/0 était en inside et l’interface se2/0 était sur outside. Il faut juste inverser les deux pour que le paquet sorte des deux routeurs :



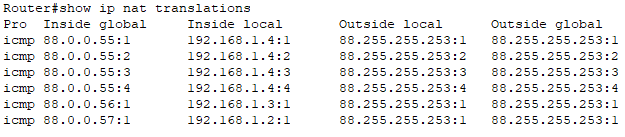
# Exercice 4 : NAT dynamique partie 1

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

Dans cette configuration, nous mettons en place la traduction d'adresses réseau (NAT) sur un routeur.La commande ip nat pool TP-POOL 88.0.0.55 88.0.0.57 netmask 255.0.0.0 définit un pool d'adresses publiques utilisables pour la traduction, allant de 88.0.0.55 à 88.0.0.57. Cela permet d'utiliser plusieurs adresses publiques. La commande access-list 1 permit 192.168.1.0 0.0.0.255 autorise uniquement les adresses du réseau privé 192.168.1.0/24 à être traduites via le NAT. Avec ip nat inside source list 1 pool TP-POOL, le NAT est appliqué en associant le pool d'adresses publiques (TP-POOL) à la liste d'accès 1. L’interface fa4/0 est définie comme l'interface interne avec ip nat inside, ce qui signifie qu'elle est du côté privé du réseau. L’interface fa0/0 est définie comme l'interface externe avec ip nat outside , ce qui signifie qu'elle est du côté public (vers Internet).

Le routeur peut maintenant traduire les adresses IP privées en adresses publiques à l'aide du pool défini. Les machines du réseau privé peuvent donc accéder à internet.



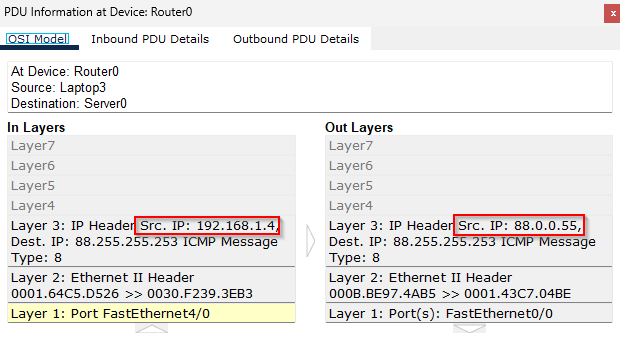
Dans cette autre capture, on voit à nouveau des traductions NAT, mais avec des adresses et des ports légèrement différents. Par exemple, 192.168.1.4:1 est traduit en 88.0.0.55:1. Ce qui est sympa ici, c’est de voir comment le routeur distribue les adresses publiques du pool (88.0.0.55 à 88.0.0.57) pour chaque appareil du réseau local. Le NAT fait tout ça de manière dynamique, ce qui permet à tout le réseau local de se connecter à Internet sans qu’il y ait de conflit.

Une image contenant texte, capture d’écran, Police, nombre

Description générée automatiquement

La commande show ip nat translation permet de voir comment le routeur traduit les adresses IP privées en adresses publiques. Par exemple, l’adresse privée 192.168.1.3:10 devient 88.0.0.55:10 lorsqu’elle sort vers Internet.

Les colonnes "Inside Local" montrent l’adresse privée originale, et "Inside Global" montre son équivalent public. Les colonnes "Outside Local" et "Outside Global" affichent l’adresse de la destination externe. Ce qui est intéressant, c’est que le NAT utilise des ports pour gérer plusieurs connexions en même temps, ce qui est pratique pour partager un petit nombre d’adresses publiques entre plusieurs appareils locaux.



On voit que dans In Layers, l’adresse IP source est 192.168.1.4, une adresse publique. Dans Out Layer, on voit que l’adresse source est 88.0.0.55, une adresse publique. Le NAT a bien traduit l’adresse privé en adresse publique avec la bonne adresse (entre 88.0.0.55 et 88.0.0.57).

# Exercice 5 : NAT dynamique partie 2 :

## Configuration du rip :



Cette capture montre une configuration RIP (Routing Information Protocol) sur un routeur. Voici les détails :

La commande router rip active le protocole de routage RIP sur le routeur. La commandes network : ajoutes des réseaux internes dans le protocole Rip pour qu’il puisse être annoncé aux autres routeurs. Cette configuration est utilisée pour permettre le routage dynamique entre les réseaux locaux et distants. RIP diffuse automatiquement les routes entre les routeurs connectés, ce qui simplifie la configuration et la gestion du routage dans des réseaux de petite ou moyenne taille. Cela garantit que les paquets peuvent être acheminés entre les réseaux 192.168.1.0 et 200.1.1.0 sans nécessiter de routes statiques.

## Configuration du nat :

Une image contenant texte, capture d’écran, Police, nombre

Description générée automatiquement

Cette capture montre la configuration du NAT (Network Address Translation) dynamique sur un routeur. La création d’un pool d’adresses NAT :la commande ip nat pool rena 200.1.1.1 200.1.1.10 netmask 255.255.255.0 configure un pool d’adresses publiques allant de 200.1.1.1 à 200.1.1.10. Ce pool sera utilisé pour traduire les adresses privées en adresses publiques La configuration d’une liste d’accès (ACL), la commande access-list 1 permit 192.168.1.0 0.0.0.255 autorise les adresses du sous-réseau 192.168.1.0/24 à utiliser le NAT. L’association de l’ACL au NAT, la commande ip nat inside source list 1 pool rena associe l’ACL à la pool d’adresses NAT. Cela permet aux adresses IP internes correspondant à l’ACL d’être traduites en adresses publiques issues du pool rena. La configuration des interfaces, int se2/0 configure l’interface externe avec ip nat outside. Cette interface est utilisée pour le trafic sortant vers Internet. int fa0/0 configure l’interface interne avec ip nat inside. Cette interface gère les adresses privées du réseau local.

Le serveur0 : 192.168.1.1

PC0 : 192.168.1.3

PC1 : 192.168.1.4

Server1 : 10.1.1.2

PC2 :10.1.1.3

PC3 : 10.1.1.4.

Les switchs n’ont pas d’adresses IP :

Une image contenant texte, Police, capture d’écran, ligne

Description générée automatiquement

Ce n’est pas dérangeant car les switchs n’ont pas besoin de communiquer avec le réseau, mais uniquement de transmettre les paquets entre les appareils connectés sur leurs ports. Ils fonctionnent au niveau 2 (couche de liaison) du modèle OSI et utilisent les adresses MAC pour acheminer les trames, ce qui ne nécessite pas d’adresse IP.Une image contenant texte, capture d’écran, logiciel, affichage

Description générée automatiquement

Il n’y a pas d’adresses configurées pour les interfaces sur le routeur, j’ai donc regardé les différentes adresses prises pour éviter tout conflit et sélectionné la dernière disponible (192.168.1.254 pour fa0/0 du router0, 200.1.1.254 pour se2/0 du router0, 10.1.1.254 pour fa0/0 du router1 et 200.1.1.253 pour le se2/0 du router1), j’ai ensuite choisi le masque de sous-réseau 255.255.255.0 car c’est en /24. J’ai aussi activé l’interface pour qu’elle soit active.

J’ai pris les dernières adresses disponibles pour les interfaces et j’ai pris les plus grandes pour les appareils de gauche.

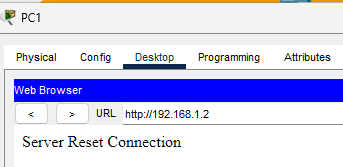
Une image contenant texte, capture d’écran, logiciel, Page web

Description générée automatiquement

La passerelle par default des postes n’est pas bonne, elle pointe sur le server0 et non les routeurs correspondants. Je l’ai donc remplacé par 192.168.1.254 et 10.1.1.254.

# Exercice 7 : NAT : redirection de ports :

Le ping réussi entre le PC1 et le serveur CISCO.FR devrait afficher le site web du serveur :



Mais ce n’est pas le cas, la tentative de connexion au serveur ne marche pas. Elle est trop lente.



Le ping (icmp) lui est bien réussi (Successful).

Une image contenant texte, capture d’écran, Police, ligne

Description générée automatiquement

Je configure du NAT statique sur le routeur pour rediriger le trafic HTTP (port 80) vers le serveur interne. Cette configuration associe l’adresse publique 132.78.241.30 au serveur interne 192.168.1.2 pour le port 80 (HTTP). Tout le trafic entrant sur l’adresse publique et ce port sera redirigé vers le serveur interne. Je rends le serveur web interne accessible depuis Internet.

Le site web s’affiche grâce au nat statique :

Une image contenant texte, capture d’écran, affichage, logiciel

Description générée automatiquement

Et le PC1 peut se connecter au site web de serverCISCO.FR. La connexion a bien été établit et grâce au dns 8.8.8.8. On a juste besoin de connaitre le nom de domaine.

J’ai configuré une route nat static sur le router cisco pour que les connections soient plus sécurisés.



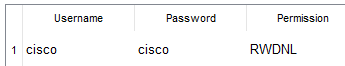
Le seul changement entre les configurations HTTP et HTTPS est les portsutilisés (port 80 pour HTTP et port 443 pour HTTPS) car les adresses IP (interne et externe) restent les mêmes. Elles représentent au serveur local hébergeant les services HTTP et HTTPS et l'interface publique du routeur.

## FTP :

Pour le protocole FTP, deux ports sont utilisés : le port 21utilisé pour établir la connexion et transmettre les commandes et le port 20utilisé pour les transferts de fichiers en mode actif. Il y aura donc deux commandes pour les deux ports :



Cette capture montre deux commandes de configuration NAT statique sur un routeur, spécifiquement pour rediriger les ports 20 et 21, qui sont utilisés pour le protocole FTP (File Transfer Protocol). Il faut se connecter à l’adresse 132.78.241.30 car on l’a configuré plus haut. De plus le FTP doit être sur une adresse publique car si on veut qu’un poste sur un autre réseau accède au ftp il doit passer par internet.



C’est l’utilisateur sur lequel on va se connecter car il a tous les droits (RWDNL).

J’ai créé un fichier a envoyé et à récupérer :

Une image contenant texte, Police, capture d’écran

Description générée automatiquement

Je l’ai ajouté sur le serveur ftp :

Une image contenant texte, Appareils électroniques, capture d’écran, ordinateur

Le contenu généré par l’IA peut être incorrect.

Cette capture montre une session FTP depuis un terminal où deux tentatives de connexion ont lieu :

Première tentative (échec), une connexion FTP est tentée vers 132.78.241.30 mais elle ne marche pas. J’ai donc essayé de me connecter avec une adresse de bouclage, la communication reste à l'intérieur de l'appareil, la communication est bien réussie.

En mode passif, la commande put coucou.txt est utilisée pour transférer le fichier coucou.txt vers le serveur FTP local. Le transfert est terminé avec succès.

Le mode passif FTP (FTP Passive Mode) est une méthode utilisée pour établir des connexions FTP où le client est responsable d’initier toutes les connexions réseau, y compris la connexion de données. Le serveur FTP ne tente pas d’établir une connexion vers le client. Au lieu de cela, le serveur FTP ouvre un port aléatoire et informe le client de ce port via la connexion de contrôle. Le mode passif fonctionne mieux dans les environnements où le client est derrière un pare-feu ou NAT, car le serveur n'initie aucune connexion vers le client.

Une image contenant texte, capture d’écran, Police

Le contenu généré par l’IA peut être incorrect.

Malheureusement une erreur est survenue lors du transfert du fichier.

Une image contenant texte, Appareils électroniques, capture d’écran, logiciel

Le contenu généré par l’IA peut être incorrect.

J’ai déjà rencontré des difficultés à me connecter au serveur ftp, pourtant le ping fonctionnait bien.

## Ajout de mon site web :

L’objectif principal de la redirection des ports est de permettre l’accès à un service hébergé en interne (dans le réseau privé) depuis l’extérieur (Internet). En appliquant cette configuration, mon site web pourra être consulté par des utilisateurs externes via un nom de domaine.

Une image contenant texte, capture d’écran, nombre, affichage

Le contenu généré par l’IA peut être incorrect.

J’ai ajouté mon site web sur le Server 0 (DNS) car le serveur cisco contenait déjà un autre site web dans son fichier index.html. Ce fichier est essentiel car il est automatiquement servi lorsqu’un utilisateur accède à la racine du site web, je n’ai donc pas remplacé pour qu’on accède quand même au site de cisco. J’ai repris mon site du TP3 car il affiche mon nom.

Une image contenant texte, capture d’écran, nombre, Parallèle

Le contenu généré par l’IA peut être incorrect.

Je l’ai ajouté dans ma configuration du DNS. Le nom de domaine « vialette.com » pointera donc vers le serveur 0.0.0.0, celui de google.

Une image contenant texte, capture d’écran, ordinateur, logiciel

Le contenu généré par l’IA peut être incorrect.

Dans cette capture, un utilisateur accède à l’adresse http://vialette.com via un navigateur web depuis un PC. La page affichée montre "Candice Vialette" avec un fond rose, ce qui confirme que le serveur web est fonctionnel et que la résolution DNS est correctement configurée.

# Exercice n°7 : Nat dynamique IPv6 en IPv4 – NAT PT

L’IPv6 (Internet Protocol version 6**)** est la dernière version du protocole Internet, conçue pour remplacer IPv4 en raison de la pénurie d’adresses IP disponibles. Contrairement à IPv4, qui utilise des adresses sur 32 bits (environ 4,3 milliards d’adresses uniques), IPv6 repose sur un adressage en 128 bits, ce qui offre un espace d’adressage presque illimité.

Une image contenant texte, capture d’écran, Police, nombre

Description générée automatiquement

Nous configurons une adresse IPv6 statique sur un périphérique. L’adresse IPv6 configurée est 2001::2/64, avec une passerelle par défaut 2001::1 et un serveur DNS 2002::808:808. Cette configuration permet au périphérique d’être connecté à un réseau IPv6, avec une communication possible via le routeur à l’adresse 2001::1.



Sur le routeur, l’interface gig0/0 est configurée avec l’adresse IPv6 2001::2/64 via la commande ipv6 address 2001::2/64, et l’interface est activée avec la commande no shutdown. Cela permet au routeur de communiquer sur ce réseau IPv6.



La configuration de l’interface gig0/1 du routeur attribue une adresse IPv4 192.168.0.1 avec un masque de sous-réseau 255.255.255.0. Là encore, l’interface est activée avec no shutdown, ce qui permet au routeur de servir de passerelle pour le réseau IPv4 correspondant.

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

Ici, nous voyons les résultats d’un test de connectivité à l’adresse IPv6 2001::1 à l’aide de la commande ping. Les réponses montrent que la communication est réussie avec 0 % de perte. Cela confirme que l’adresse IPv6 configurée et la passerelle fonctionnent correctement, assurant ainsi une connectivité sur le réseau IPv6.

Une image contenant texte, capture d’écran, Police, algèbre

Description générée automatiquement

Dans cette configuration, le NAT IPv6 vers IPv4 est mis en place sur le routeur. La commande ipv6 nat prefix 2002::/96 crée un préfixe qui sera utilisé pour mapper des adresses IPv4 vers des adresses IPv6. Ce préfixe est essentiel pour permettre la traduction entre les deux protocoles. La liste d’accès v6\_to\_v4\_acl autorise le trafic provenant du réseau IPv6 2001::/64 vers n’importe quelle destination (any). Cela limite la portée du NAT à ce réseau source. La commande ipv6 nat v6v4 source list v6\_to\_v4\_acl interface gig0/1 overload met en place la traduction pour les paquets IPv6 correspondant à l’ACL. L’interface gig0/1 est utilisée comme interface de sortie pour les traductions. La commande ipv6 unicast-routing active le routage IPv6, et ip route 0.0.0.0 0.0.0.0 gig0/1 ajoute une route par défaut pour le trafic IPv4. Cela permet au routeur de rediriger tout le trafic IPv4 vers l’interface gig0/1.

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

Une configuration similaire est appliquée, mais avec des listes d’accès et des interfaces légèrement différentes, confirmant une approche cohérente pour gérer le NAT IPv6 vers IPv4.



Les commandes finales activent le routage unicast IPv6 et ajoutent une route IPv4 par défaut, ce qui est crucial pour assurer une connectivité complète entre les deux protocoles.

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

Le test de ping vers l’adresse IPv6 2001::1 montre une communication réussie, avec 0 % de perte. Cela confirme que la configuration NAT et le routage IPv6 fonctionnent correctement, permettant une communication entre les appareils configurés sur ce réseau.

Une image contenant texte, capture d’écran, nombre, Police

Le contenu généré par l’IA peut être incorrect.

J’ai défini mes paramètres sur l’enveloppe ICMP pour qu’elle prenne en compte l’ipv6 au lieu de l’ipv4.

Paramètres :

* Source Device: PC0 est l’appareil émettant le test.
* Outgoing Port : Le port utilisé est automatiquement sélectionné.
* Select Application : PING, utilisé pour vérifier la connectivité réseau
* Destination IP Address : 2001::1, une adresse IPv6 à qui on veut envoyer le ping.
* Source IP Address : automatiquement rempli par l’appareil émetteur en fonction de sa configuration IP.
* TTL : 32, la durée de vie maximale d’un paquet avant qu’il ne soit abandonné, limitant les sauts (hops) autorisés.
* TOS (Type of Service) : 0, utilisé pour spécifier la priorité ou le traitement des paquets.
* Sequence Number : 1, indique qu’il s’agit du premier paquet dans une séquence de tests.
* Size : 110, la taille du paquet, en octets.
* One Shot : Le test sera exécuté une seule fois après un délai de 2 secondes.
* Periodic : Non sélectionné ici, mais permettrait d’exécuter le test régulièrement à intervalles définis.

L’enveloppe ICMP est maintenant réussite :

Une image contenant texte, capture d’écran, Police, ligne

Le contenu généré par l’IA peut être incorrect.

# Modification de notre réseau :

## Création des différents réseaux :

J’ai choisi les différents réseaux :

* Le réseau rouge pour l’administration car il est dans le réseau interne et sert pour administrer tout mon réseau.
* Le réseau vert servira de sous-réseau serveur car il n’a pas de spécificité.
* Le réseau bleu sera la zone démilitarisée car il contient le site web. Si un hackeur arrive à pirater notre serveur, il ne pourra pas avoir accès au reste de notre réseau.
* Le réseau jaune restera le sous-réseau des postes utilisateur dans le magasin.

Une image contenant texte, carte, diagramme, capture d’écran

Description générée automatiquement

J’ai rajouté un réseau car j’avais un réseau magasin mais réservé pour le magasin (wifi) et non pour l’entreprise.

### Les nouvelles adresses IP :

|  |  |  |
| --- | --- | --- |
| **Appareils** | Adresse IP | Passerelle par default |
| **Server WEB invite** | 10.2.29.1 |  |
| **PC1** | 10.2.29.2 |  |
| **Server web et HTTP** | 10.9.29.1 | 172.16.1.1 |
| **Serveur DNS, DHCP et AAA** | 10.1.29.1 | 10.1.29.253 |
| **Serveur Messagerie** | 10.1.29.2 | 10.1.29.253 |
| **Serveur FTP** | 10.1.29.3 | 10.1.29.253 |
| **Serveur TFTP** | 10.3.29.2 | 10.3.29.254 |
| **Serveur Log** | 10.3.29.3 | 10.3.29.254 |
| **HP181** | 10.3.29.4 | 10.3.29.254 |
| **PC\_admin** | 10.3.29.1 | 10.3.29.254 |
| **Firewall fa 0/0** | 172.16.1.1 |  |
| **Firewall gig 0/1** | 10.9.29. 254 |  |
| **RO\_EXT\_INT gig0/0** | 10.9.29. 253 |  |
| **RO\_EXT\_INT gig0/1** | 10.1.29.254 |  |
| **RO\_INT\_INT gig0/0** | 10.1.29.253 |  |
| **RO\_INT\_INT gig0/1** | 10.3.29.254 |  |
| **WRT300N** | 192.168.29.254 | 172.16.1.1 |
| **RO\_EXT\_INT gig0/2** | 10.2.29.254 |  |

### Modification des noms/adresses IP :

Une image contenant texte, capture d’écran, Police, nombre

Description générée automatiquement

Dans Config, puis global, on peut changer le nom des dispositifs dans le champ display Name.



On configure l’adresse IP des interfaces grâce à la commande ip address. Cela permet que les routeurs puissent communiquer entre eux.

Une image contenant texte, capture d’écran, logiciel, affichage

Description générée automatiquement

Je configure l’adresse IP

## Routage :

Le protocole RIP (Routing Information Protocol) est un protocole de routage à vecteur de distance utilisé pour échanger des informations de routage entre les routeurs d’un réseau. Il fonctionne sur le principe du comptage de sauts , où chaque routeur transmet périodiquement la liste des routes qu’il connaît à ses voisins.

Je supprime le routage ospf, il n’est plus à jour avec les adresses IP qui ont changé.



Je configure à la place du rip, plus facile a mettre en place et convenant très bien à un réseau de petite taille :

Une image contenant texte, Police, reçu, ligne

Le contenu généré par l’IA peut être incorrect.

Cette capture montre la configuration d’un routeur rip. router rip active le protocole rip sur le routeur et network 10.9.29.0, network 10.2.29.0, et network 10.1.29.0 ajoutent ces réseaux au protocole RIP pour qu’ils puissent être annoncés et appris dynamiquement par les autres routeurs.

## Serveur DNS, DHCP et AAA :

### DNS :

Le DNS (Domain Name System) est un système essentiel qui permet de traduire les noms de domaine en adresses IP. En effet, les utilisateurs accèdent aux sites web en tapant des adresses faciles à retenir ([www.google.com](http://www.google.com)), mais les machines communiquent entre elles via des adresses IP. Grâce au DNS, un ordinateur peut interroger un serveur DNS pour obtenir l’adresse IP associée à un nom de domaine.

Une image contenant texte, capture d’écran, nombre, Police

Le contenu généré par l’IA peut être incorrect.

On désactive le service DNS qui était sur le serveur http pour le mettre uniquement sur le serveur DNS.

Une image contenant texte, capture d’écran, nombre, Police

Le contenu généré par l’IA peut être incorrect.

J’active le service DNS et rajoute mon nom de domaine avec l’adresse IP du serveur qui l’héberge pour taper juste mon nom de domaine et accéder à mon site web.

### DHCP :

Le protocole DHCP (Dynamic Host Configuration Protocol) est un protocole réseau qui permet d’attribuer automatiquement des adresses IP et d’autres paramètres de configuration aux appareils connectés à un réseau. Sans DHCP, il faudrait attribuer manuellement une adresse IP à chaque machine, ce qui serait fastidieux et source d’erreurs. Avec DHCP, un serveur attribue dynamiquement une adresse IP à un appareil pour une durée déterminée (appelée bail). Ce protocole peut également fournir d’autres informations essentielles comme le masque de sous-réseau, la passerelle par défaut et les adresses des serveurs DNS. Il simplifie considérablement l’administration des réseaux, notamment dans les grandes infrastructures où les connexions et déconnexions d’appareils sont fréquentes.

Une image contenant texte, capture d’écran, nombre, affichage

Le contenu généré par l’IA peut être incorrect.

Cette capture présente la configuration du service DHCP pour l’interface FastEthernet0. Pool Name pour indiquer le nom du pool d’adresses IP, Default Gateway : 10.9.29.254 pour définir la passerelle par défaut pour les clients, le DNS Server: 10.1.29.1 qui spécifie le serveur DNS pour la résolution des noms de domaine, Start IP Address : 10.9.29.0 qui définit la première adresse IP attribuable du pool, Subnet Mask : 255.255.255.0 qui détermine la taille du sous-réseau, Maximum Number of Users : 256 qui indique le nombre maximal d’utilisateurs pouvant recevoir une adresse IP et le TFTP Server : 10.3.29.2, utilisé pour le transfert de fichiers réseau.

J’ai défini le maximum d’utilisateurs à 15 ça permet de réduire les risques de connexions non autorisées. De plus si dans le futur, j’ajoute des utilisateurs ou des appareils, il sera plus facile d'étendre la plage DHCP sans modifier les configurations actuelles.

Une image contenant texte, capture d’écran, Police, ligne

Le contenu généré par l’IA peut être incorrect.

J’ai aussi exclu les adresses IP de 10.2.29.16 à 10.2.29.254 pour limiter le nombre d’adresses IP attribuable.

****

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |

Ip helper-address permet de traverser les segments réseau et d'atteindre une destination située sur un autre sous-réseau. Le DHCP étant dans un autre sous-réseau, les appareils ne pourraient pas atteindre le DHCP.

### AAA :

Le concept AAA (Authentication, Authorization, and Accounting) regroupe trois fonctions essentielles dans la gestion de la sécurité des réseaux et des systèmes informatiques. L’authentification (Authentication) consiste à vérifier l’identité d’un utilisateur ou d’un appareil à l’aide d’identifiants comme un mot de passe, une carte à puce ou un certificat. L’autorisation (Authorization) détermine les ressources auxquelles un utilisateur a accès en fonction de son rôle ou de ses permissions. Enfin, l’accounting (comptabilité) enregistre et surveille l’activité des utilisateurs, ce qui permet de générer des journaux d’audit et de facturation. AAA est utilisé dans divers systèmes, notamment dans les accès aux réseaux d’entreprise via des protocoles comme RADIUS et TACACS+, ou encore pour gérer les accès aux services cloud.

Le réseau est fait pour environ 10 utilisateurs. 8 dans le magasin et deux dans l’administration.

Je créé donc 10 utilisateurs pour mes serveurs AAA et messagerie :

Candice VIALETTE (pdg) PC\_admin

Eloham CARON (Responsable Sécurité)

Bruno DROGUE (Responsable IT)

Jean-Maxime RIEDEL (Directeur Financier)

Martine Henard (Responsable Marketing)

Eriam Shaffter (Chef de Projet)

Samuel GIBERT (Développeur Web)

Alice MOREL (Responsable RH)

Sébastien RODRIGUEZ (secrétaire comptable)

Sophie LEBRUN (Employé Caisse) PC 1

Sophie et Candice sont les seules à avoir un poste avec une adresse IP fixe. Le serveur AAA a besoin d’une IP fixe car si elle change, l’utilisateur ne pourra plus se connecter via son poste.

Une image contenant texte, capture d’écran, nombre, Police

Le contenu généré par l’IA peut être incorrect.

Configuration du client RADIUS :

* Client Name : vialette (ou lebrun).
* Client IP : 10.3.29.1, indiquant l’adresse IP de l’appareil qui utilisera le serveur RADIUS pour s’authentifier.
* Secret : candice, qui est la clé partagée utilisée pour sécuriser la communication entre le client et le serveur RADIUS.

J’ai choisi le serveur Radius car il convient parfaitement à un environnement hétérogène comme celui-ci, où plusieurs types d’appareils sont connectés, tels que des ordinateurs, des smartphones et des imprimantes. Il est particulièrement utile pour gérer l’authentification des utilisateurs finaux dans des services réseau comme le Wi-Fi, les VPN ou encore PPPoE, ce qui correspond aux besoins des segments comme le Magasin ou les Utilisateurs.

De plus, il utilise le protocole UDP, qui est moins gourmand en ressources que TCP utilisé par TACACS+. Cela représente un avantage non négligeable dans ce réseau où certains équipements, comme les points d’accès et les petits routeurs, pourraient avoir des ressources limitées. En choisissant RADIUS, je peux également centraliser la gestion de l’authentification et des droits d’accès sur l’ensemble des sous-réseaux (Magasin, Utilisateurs, Administration, DMZ, Serveurs), ce qui simplifie énormément la gestion globale du réseau. Par ailleurs, RADIUS permet de suivre l’activité des utilisateurs grâce à sa fonction d’accounting, ce qui est utile, par exemple, pour surveiller l’utilisation des services Wi-Fi dans le Magasin.

## Serveur FTP :

Une image contenant texte, nombre, ligne, Parallèle

Le contenu généré par l’IA peut être incorrect.Un serveur FTP est un système permettant de stocker et de partager des fichiers à distance via le protocole FTP (File Transfer Protocol). Il permet aux utilisateurs d’envoyer ou de récupérer des fichiers en se connectant à distance à l’aide d’un client FTP.

Cette capture montre la configuration d’un serveur FTP avec des utilisateurs et des permissions spécifiques. Voici une justification pour chaque utilisateur et les permissions attribuées en fonction de leur rôle :

1. Candice Vialette :  
   Permissions : RWDNL (Read, Write, Delete, Rename, List), car en tant que PDG, elle a besoin d’un accès complet pour consulter, modifier, et gérer les fichiers critiques de l’entreprise.
2. Eloham Caron (Responsable Sécurité) :  
   Permissions : RW (Read, Write) car il doit pouvoir lire et modifier les fichiers nécessaires à la sécurité, mais il n’est pas autorisé à les supprimer pour éviter les erreurs ou abus.
3. Bruno Drogue (Responsable IT) :  
   Permissions : RW (Read, Write) car en tant que responsable IT, il a besoin de modifier les fichiers techniques ou de configuration, mais pas nécessairement de les supprimer.
4. Jean-Maxime Riedel (Directeur Financier) :  
   Permissions : R (Read) car il peut consulter les fichiers financiers pour ses analyses, mais aucune modification ou suppression n’est autorisée pour préserver l’intégrité des données.
5. Martine Henard (Responsable Marketing) :  
   Permissions : R (Read) car elle peut accéder aux fichiers nécessaires pour le marketing, mais pas les modifier ou supprimer pour éviter les risques de perte de données.
6. Eriam Shaffter (Chef de Projet) :  
   Permissions : RW (Read, Write) car elle a besoin de modifier les fichiers liés aux projets pour assurer leur mise à jour et leur suivi.
7. Samuel Gibert (Développeur Web) :  
   Permissions : R (Read) car il doit pouvoir consulter les fichiers nécessaires à son développement sans les modifier directement pour éviter les erreurs.
8. Alice Morel (Responsable RH) :  
   Permissions : R car un accès limité aux fichiers nécessaires pour consulter des informations RH.
9. Sébastien Rodriguez (Secrétaire Comptable) :  
   Permissions : R car un accès limité pour consulter les fichiers comptables et administratifs.
10. Sophie Lebrun (Employée Caisse) :  
    Permissions :aucun accès car son métier ne nécessite pas d’accès au serveur FTP.

## Serveur Messagerie :

L’email est un moyen de communication numérique permettant d’envoyer des messages textuels, des pièces jointes et d’autres types de données via Internet. Il fonctionne grâce à plusieurs protocoles comme SMTP (Simple Mail Transfer Protocol) pour l’envoi des emails, ainsi que POP3 (Post Office Protocol) pour la récupération des messages depuis un serveur distant. Chaque utilisateur possède une adresse email unique associée à une boîte aux lettres hébergée sur un serveur.

### Configuration :

Une image contenant texte, capture d’écran, affichage, logiciel

Description générée automatiquement

Cette capture montre la configuration d’un service de messagerie sur un serveur. Les services SMTP et POP3 sont activés pour le domaine vialette.com. Les utilisateurs sont configurés avec leurs identifiants, par exemple, l’utilisateur drogue avec le mot de passe bruno. Cette configuration permet aux utilisateurs de recevoir (POP3) et d’envoyer (SMTP) des e-mails via ce serveur.

Une image contenant texte, capture d’écran, nombre, Police

Le contenu généré par l’IA peut être incorrect.

J’ai aussi ajouté un nom de domaine pour « vialette.com » car il dirige les e-mails d’un domaine vers les serveurs hébergeant les comptes de messagerie des utilisateurs.

Une image contenant texte, capture d’écran, nombre, Police

Le contenu généré par l’IA peut être incorrect.

La configuration de la messagerie sur le PC3 montre que l’adresse e-mail de l’utilisateur drogue@vialette.com est paramétrée avec les serveurs de messagerie :

* Serveur entrant (Serveur Messagerie) : 10.1.29.2
* Serveur sortant (Serveur Messagerie) : 10.1.29.2  
  Les identifiants de connexion incluent l’adresse e-mail et le mot de passe associé. Cela permet à l’utilisateur d’envoyer et de recevoir des e-mails en utilisant le service de messagerie configuré sur le serveur.

### Test :

Une image contenant texte, capture d’écran, Police, affichage

Le contenu généré par l’IA peut être incorrect.

Un test d’envoi de mail a été effectué depuis le serveur vers l’adresse drogue@vialette.com avec le sujet "Test". L’e-mail a été envoyé avec succès en utilisant le serveur de messagerie situé à l’adresse IP 10.1.29.2.

Une image contenant texte, Appareils électroniques, capture d’écran, logiciel

Le contenu généré par l’IA peut être incorrect.

Mais il y a une erreur de résolution de DNS, je n’est pas réussi a la corriger.

## Serveur TFTP :

Le TFTP (Trivial File Transfer Protocol) est une version simplifiée du protocole FTP, conçue pour transférer des fichiers de manière rapide et efficace, mais avec des fonctionnalités réduites. Contrairement au FTP classique, il ne nécessite pas d’authentification et utilise le protocole UDP (User Datagram Protocol) au lieu de TCP, ce qui le rend plus léger mais aussi moins fiable, car il ne garantit pas la retransmission des paquets en cas de perte.

Une image contenant texte, capture d’écran, Police, document

Le contenu généré par l’IA peut être incorrect.

Cette capture montre la sauvegarde et la restauration (test) de la configuration d’un routeur via un serveur TFTP :

Sauvegarde de la configuration courante sur un serveur TFTP :

* + La commande copy running-config tftp est utilisée pour copier la configuration active vers un serveur TFTP.
  + Adresse du serveur TFTP : 10.3.29.2.
  + Nom du fichier destination : firewall-config (remplacer firewall par le nom du routeur)

La configuration est sauvegardée avec succès sur le serveur TFTP (taille : 1307 octets).

Je veux tester si le serveur tftp a bien enregistré les configurations :

Restauration de la configuration depuis un serveur TFTP vers la mémoire flash :

* + La commande copy tftp: flash: est utilisée pour copier le fichier depuis le serveur TFTP vers la mémoire flash du pare-feu.
  + Adresse du serveur TFTP : 10.3.29.2.
  + Fichier source : firewall-config.

Le fichier est récupéré depuis le serveur TFTP et sauvegardé localement sur le pare-feu.

Une image contenant texte, capture d’écran, logiciel, affichage

Le contenu généré par l’IA peut être incorrect.

Dans le service TFTP du serveur, on voit bien les 3 fichiers qu’on a configuré.

Cette méthode garantit que la configuration actuelle est sécurisée sur un serveur externe, en cas de redémarrage ou de panne du pare-feu. Le transfert de la configuration depuis le TFTP vers la mémoire flash permet de recharger rapidement les paramètres en cas de besoin, comme après une réinitialisation ou un remplacement de matériel. L’utilisation du protocole TFTP est courante pour des sauvegardes rapides dans des environnements réseau, car il est simple et efficace pour transférer des fichiers de configuration.

## Serveur log :

Le log désigne l’enregistrement des événements et des actions effectuées sur un système informatique ou un réseau. Ces fichiers de journalisation permettent aux administrateurs de suivre l'activité des utilisateurs, d’analyser les erreurs et de détecter d’éventuelles tentatives d’intrusion ou de dysfonctionnements.



Je redirige les logs vers le serveur des logs (10.3.29.3) pour qu’ils puissent être tous au même endroit. Ça sera plus simple à surveiller pour des administrateur système.

## Routeur WRT300N :

Une image contenant texte, capture d’écran, nombre, affichage

Le contenu généré par l’IA peut être incorrect.

J’ai changé le DHCP pour qu’il attribue les nouvelles adresses IP de 192.168.29.1 à 192.168.29.15, un nouveau DNS, 10.1.29.1 et un maximum d’utilisateur à 15 pour ajouter des postes si besoin et rendre moins d’adresses disponibles.

Une image contenant texte, capture d’écran, nombre, Police

Le contenu généré par l’IA peut être incorrect.

Cette capture montre une configuration réseau où une adresse IP statique est définie pour un appareil. Voici les détails de la configuration :

1. Type de connexion Internet :
   * La connexion est définie en mode Static IP, ce qui signifie que les paramètres IP sont configurés manuellement et ne changent pas.
2. Paramètres réseau :
   * Internet IP Address : 192.168.29.254 est l’adresse IP de l’appareil sur le réseau.
   * Subnet Mask **:** 255.255.255.0 est le masque de sous-réseau
   * Default Gateway : 172.16.1.1 est l’adresse IP de la passerelle utilisée pour accéder aux autres réseaux, notamment Internet.
   * DNS 1 : 10.1.29.1 est l’adresse du serveur DNS utilisé pour la résolution de noms de domaine.

## Mise en place du NAT/PAT :

Dans ce réseau, la mise en place du NAT et du PAT est essentielle pour garantir une communication efficace et sécurisée entre les différents segments internes et l’extérieur, tout en optimisant les ressources IP disponibles.

Premièrement, le NAT est crucial pour permettre aux machines utilisant des adresses privées d’accéder à Internet via une adresse publique unique. Étant donné que les plages d’adresses privées définies par la RFC 1918 ne sont pas routables sur Internet, le NAT traduit ces adresses internes en une adresse publique visible sur Internet. Cela permet à tous les utilisateurs du réseau interne (ordinateurs, smartphones, serveurs) d’accéder aux ressources externes.

Ensuite, l’utilisation du PAT est justifiée pour optimiser l’utilisation de l’adresse IP publique allouée. Dans un contexte où plusieurs hôtes internes accèdent simultanément à Internet, le PAT permet d’utiliser une seule adresse publique en différenciant les connexions grâce aux numéros de ports. Par exemple, les PC du segment utilisateur (10.2.29.0) peuvent partager une adresse IP publique unique lorsqu’ils naviguent sur le web ou utilisent d’autres services en ligne, sans nécessiter une adresse publique pour chaque appareil.

De plus, la mise en place du NAT statique peut être utile pour rendre accessibles certains serveurs internes depuis l’extérieur. Par exemple, le serveur web situé dans la DMZ (10.9.29.0) pourrait être accessible publiquement via une adresse IP publique statique. Cela garantirait que les utilisateurs externes puissent consulter les pages web hébergées tout en sécurisant l’accès grâce à des règles spécifiques sur le pare-feu.

Enfin, le NAT et le PAT jouent un rôle dans l’isolation des segments réseau. Chaque segment du réseau a une fonction spécifique (serveurs, utilisateurs, DMZ, administration), et le NAT permet de limiter les flux entre ces segments et l’extérieur, en définissant clairement quelles ressources sont accessibles et par quel chemin. Cela renforce également la sécurité globale du réseau en masquant les adresses IP internes et en filtrant les connexions entrantes non autorisées.

Une image contenant texte, Police, capture d’écran, blanc

Le contenu généré par l’IA peut être incorrect.

Dans cette configuration, l’interface se2/0 du pare-feu est définie comme une interface NAT externe :

1. ip nat outside : Configure l’interface comme étant le point de sortie vers l’extérieur du réseau.
2. no shutdown **:** Active l’interface, la rendant opérationnelle.

Elle redirigera les paquets vers l’extérieur du réseau.

Une image contenant texte, Police, blanc, algèbre

Le contenu généré par l’IA peut être incorrect.

L’interface fa1/0 est configurée comme une interface NAT interne car elle est à l’intérieur du réseau.

Une image contenant texte, capture d’écran, Police, ligne

Le contenu généré par l’IA peut être incorrect.

Listes d’accès (ACL) :

* Les commandes access-list 1 permit autorisent les sous-réseaux 10.9.29.0, 10.1.29.0, 10.3.29.0 et 10.2.29.0 à utiliser la traduction d’adresses (NAT).
* Ces ACL limitent le NAT aux réseaux internes spécifiés.

NAT Overload :

* La commande ip nat inside source list 1 interface se2/0 overload met en place un NAT dynamique avec surcharge sur l’interface externe se2/0.
* Cela permet à plusieurs appareils internes d’utiliser une seule adresse IP publique en associant des ports uniques à chaque connexion.

Cette configuration est idéale pour permettre aux réseaux internes de communiquer avec l’extérieur en utilisant une seule adresse publique (interface se2/0). La surcharge NAT optimise l’utilisation des adresses publiques pour 1 seule adresse contre 10 fois plus si toutes les adresses étaient publiques.

## Points forts du réseau :

L’architecture mise en place repose sur une séparation des réseaux par fonction, ce qui améliore la sécurité et l’organisation des ressources. La segmentation en quatre sous-réseaux distincts (serveurs, production, administration et DMZ) permet une gestion plus efficace du trafic réseau et une meilleure protection contre les attaques potentielles. Grâce à cette organisation, il est possible de restreindre les accès et de limiter les communications entre les différentes zones selon les besoins spécifiques.

L’utilisation des protocoles standards tels que DHCP, DNS, AAA, NAT/PAT et RIP facilite l’interconnexion et la gestion des services réseau. Chaque appareil peut être configuré dynamiquement grâce au DHCP, tandis que le DNS assure une résolution rapide des noms de domaine internes. Le protocole AAA (Authentication, Authorization, Accounting) permet un contrôle précis des utilisateurs et de leurs accès aux ressources du réseau, renforçant ainsi la sécurité globale.

L’intégration d’une DMZ (zone démilitarisée) constitue un autre point fort du réseau. Cette zone isolée est utilisée pour héberger le serveur web, rendant l’infrastructure plus résistante aux attaques externes. Grâce à cette configuration, même en cas de compromission du serveur web, les autres sous-réseaux critiques (comme les serveurs internes et l’administration) restent protégés.

La gestion centralisée des services contribue à réduire la complexité du réseau. Le serveur DNS joue un rôle clé en hébergeant également les services DHCP et AAA, ce qui évite la dispersion des ressources et simplifie l’administration. Cette approche permet également une gestion plus homogène des politiques de sécurité et une meilleure synchronisation des services.

L’adressage IP est bien structuré, avec des plages d’adresses bien définies pour chaque sous-réseau. Cette organisation facilite la maintenance et permet d’éviter les conflits d’adresses IP. Elle garantit également une meilleure évolutivité du réseau en cas de besoin d’extension.

## Points faibles du réseau :

Bien que la segmentation des réseaux améliore la sécurité, certains aspects doivent être renforcés. En premier lieu, l’ajout de pare-feux (ACLs plus restrictives sur les routeurs) permettrait de mieux contrôler les flux entre les différents sous-réseaux et de limiter les communications non nécessaires. Par exemple, seuls les services essentiels devraient être accessibles depuis l’extérieur via des règles spécifiques de filtrage.

Un contrôle d’accès plus strict sur les services critiques comme le FTP, les bases de données et les services AAA doit être mis en place. L’authentification multi-facteurs (MFA) pourrait être une solution supplémentaire pour renforcer la protection des comptes les plus sensibles.

L’ajout d’un IDS/IPS (Intrusion Detection System/Intrusion Prevention System) permettrait de détecter et bloquer automatiquement les tentatives d’intrusion. En analysant en temps réel le trafic réseau et les journaux des pare-feux, un IDS peut identifier des comportements suspects, tandis qu’un IPS peut prendre des mesures correctives pour empêcher une attaque.

# Conclusion :

À l’issue de ce TP, nous avons pu approfondir notre compréhension et notre maîtrise du NAT et de la redirection des ports, des technologies essentielles pour la gestion des réseaux modernes. Nous avons configuré et testé différentes formes de NAT (statique, dynamique et PAT), observant ainsi leur rôle dans la translation des adresses IP privées en adresses publiques et leur impact sur la connectivité réseau.

L’implémentation de la redirection des ports nous a permis de comprendre comment exposer des services internes, tels qu’un serveur web, tout en garantissant un certain niveau de sécurité. Nous avons également vu l’importance des listes de contrôle d’accès (ACL) et des règles de pare-feu pour limiter les accès non autorisés et sécuriser les échanges entre le réseau interne et Internet.

Ce TP nous a offert une mise en situation concrète, proche des environnements professionnels, où l’optimisation de l’adressage IP et la sécurisation des services réseau sont des enjeux majeurs. En réalisant des tests et en analysant les traductions NAT, nous avons acquis les compétences nécessaires pour configurer et dépanner des architectures réseau utilisant le NAT.

En conclusion, ce travail nous a permis de mieux comprendre les défis et les solutions liés à la connectivité des réseaux privés avec l’extérieur, en combinant fonctionnalité, performance et sécurité. Ces compétences sont indispensables pour administrer et sécuriser des infrastructures réseau dans un cadre professionnel.

# Sources :

<https://www.cisco.com/c/en/us/support/docs/ip/network-address-translation-nat/13772-12.html>

<https://fr.wikipedia.org/wiki/Liste_de_ports_logiciels>

TP4 (suivi de la connectivité)

Fiches ressources

<https://www.cisco.com/c/en/us/td/docs/ios/ios_xe/ipv6/configuration/guide/ip6-nat_trnsln_xe.html>

<https://datatracker.ietf.org/doc/html/rfc6052>

<https://fr.wikipedia.org/wiki/Courrier_%C3%A9lectronique>

<https://fr.wikipedia.org/wiki/Trivial_File_Transfer_Protocol>

<https://fr.wikipedia.org/wiki/FTP>

<https://www.fortinet.com/fr/resources/cyberglossary/aaa-security>

<https://help.openhost-network.com/hc/fr/articles/115002903945-Domaine-de-messagerie-Les-fondamentaux>

<https://computernetworking747640215.wordpress.com/2018/07/05/configuring-a-mail-server-in-packet-tracer/>