Exercice PT 7.2.8 : évolutivité des réseaux avec NAT

Diagramme de topologie

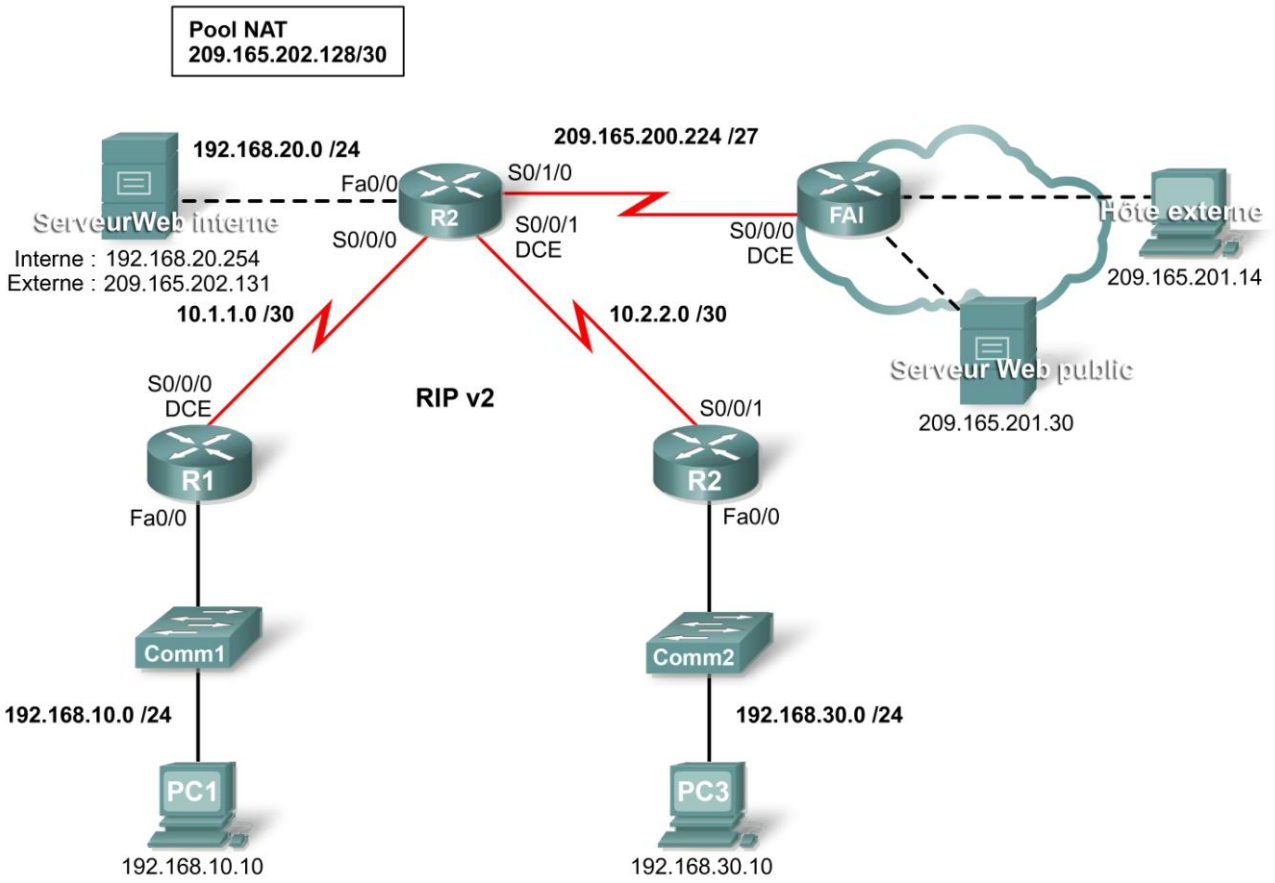

Table d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau
R1	**Fa0/1**	192.168.10.1	255.255.255.0
	S0/0/0	10.1.1.1	255.255.255.252
R2	**Fa0/0**	192.168.20.1	255.255.255.0
	S0/0/0	10.1.1.2	255.255.255.252
	S0/0/1	10.2.2.1	255.255.255.252
	S0/1/0	209.165.200.225	255.255.255.224
R3	**Fa0/1**	192.168.30.1	255.255.255.0
	S0/0/0	10.2.2.2	255.255.255.252

Suite de la table d'adressage sur la page suivante

Table d'adressage (suite)

Serveur Web interne	**Carte réseau**	Local : 192.168.20.254	255.255.255.252
	Carte réseau	Global : 209.165.202.131	255.255.255.252
PC1	**Carte réseau**	192.168.10.10	255.255.255.0
PC3	**Carte réseau**	192.168.30.10	255.255.255.0
Hôte externe	**Carte réseau**	209.165.201.14	255.255.255.240
Serveur Web public	**Carte réseau**	209.265.201.30	255.255.255.240

Objectifs pédagogiques

- Configurer une liste de contrôle d'accès pour autoriser la fonction NAT
- Configurer une fonction NAT statique
- Configurer une surcharge NAT dynamique
- Configurer le routeur FAI avec une route statique
- Tester la connectivité

Présentation

La fonction NAT traduit des adresses internes, privées et non routables en adresses publiques routables. Un avantage supplémentaire de la fonction NAT est d'offrir confidentialité et sécurité à un réseau en masquant les adresses IP internes aux réseaux externes. Au cours de cet exercice, vous allez configurer la fonction NAT statique et dynamique.

Tâche 1 : configuration d'une liste de contrôle d'accès pour autoriser la fonction NAT

Étape 1. Création d'une liste de contrôle d'accès standard nommée

Pour définir les adresses internes qui sont traduites en adresses publiques dans le processus NAT, créez une liste de contrôle d'accès standard nommée appelée R2NAT. Cette liste est utilisée dans les étapes suivantes de configuration de la fonction NAT.

```
R2(config)#ip access-list standard R2NAT
R2(config-std-nacl)# permit 192.168.10.0 0.0.0.255
R2(config-std-nacl)# permit 192.168.20.0 0.0.0.255
R2(config-std-nacl)# permit 192.168.30.0 0.0.0.255
```

Étape 2. Vérification des résultats

Votre taux de réalisation doit être de 11 %. Si ce n'est pas le cas, cliquez sur **Check Results** pour identifier les composants nécessaires qui ne sont pas complets.

Tâche 2 : configuration d'une fonction NAT statique

Étape 1. Configuration d'une fonction NAT statique pour un serveur Web interne

Le serveur Web interne doit posséder une adresse IP publique qui ne change jamais afin qu'un accès soit possible de l'extérieur du réseau. La configuration d'une adresse NAT statique permet de configurer le serveur Web avec une adresse interne privée. Le processus NAT mappe alors toujours sur l'adresse privée les paquets utilisant l'adresse publique du serveur.

```
R2(config)#ip nat inside source static 192.168.20.254 209.165.202.131
```

Étape 2. Vérification des résultats

Votre taux de réalisation doit être de 22 %. Si ce n'est pas le cas, cliquez sur **Check Results** pour identifier les composants nécessaires qui ne sont pas complets.

Tâche 3 : configuration d'une surcharge NAT dynamique

Outre l'adresse IP publique attribuée au serveur Web interne, FAI vous a attribué trois adresses publiques. Ces adresses sont mappées sur tous les autres hôtes internes qui accèdent à Internet.

Pour autoriser plus de trois hôtes internes à accéder simultanément à Internet, configurez une surcharge à la fonction NAT pour accepter les hôtes supplémentaires. La surcharge NAT, également appelée traduction d'adresses réseau (PAT, Port Address Translation), utilise les numéros de port pour faire la distinction entre les paquets des différents hôtes auxquels la même adresse IP publique a été attribuée.

Étape 1. Définition du pool d'adresses et configuration de la fonction NAT dynamique

Saisissez les commandes suivantes pour configurer le pool d'adresses publiques qui sont dynamiquement mappées sur les hôtes internes.

La première commande définit le pool de trois adresses publiques qui sont mappées sur des adresses internes.

La seconde commande indique au processus NAT le mappage des adresses dans le pool d'adresses définies dans la liste d'accès que vous avez créée à la tâche 1.

```
R2(config)#ip nat pool R2POOL 209.165.202.128 209.165.202.130 netmask
255.255.255.252
R2(config)#ip nat inside source list R2NAT pool R2POOL overload
```

Étape 2. Configuration des interfaces sur R2 pour appliquer la fonction NAT

Dans le mode de configuration d'interface sur R2, configurez chaque interface à l'aide de la commande **ip nat** {**inside** | **outside**}**.** Étant donné que les adresses internes se trouvent sur des réseaux connectés aux interfaces Fa0/0, Serial 0/0/0 et Serial0/0/1, utilisez la commande **ip nat inside** pour configurer ces interfaces. Internet étant connecté à Serial0/1/0, utilisez la commande **ip nat outside** sur cette interface.

Étape 3. Vérification des résultats

Votre taux de réalisation doit être de 89 %. Si ce n'est pas le cas, cliquez sur **Check Results** pour identifier les composants nécessaires qui ne sont pas complets.

Tâche 4 : configuration de FAI avec une route statique

Étape 1. Configuration de FAI avec une route statique vers R2

FAI nécessite une route statique vers les adresses publiques de R2. Pour cela, utilisez la commande suivante :

```
FAI(config)#ip route 209.165.202.128 255.255.255.224 serial0/0/0
```

Étape 2. Vérification des résultats

Votre taux de réalisation doit être de 100 %. Si ce n'est pas le cas, cliquez sur **Check Results** pour identifier les composants nécessaires qui ne sont pas complets.

Tâche 5 : test de la connectivité

Vous devez maintenant être en mesure d'envoyer une requête ping de tout hôte interne vers l'hôte externe ou vers le serveur Web public.

Pour visualiser les effets de NAT sur un paquet spécifique, passez en mode Simulation et observez le paquet qui provient de PC1.

Cliquez sur la zone d'informations en couleur associée à ce paquet lorsqu'il passe de R1 à R2. Si vous cliquez sur **Inbound PDU Details**, vous devez voir que l'adresse source est 192.168.10.10. En cliquant sur **Outbound PDU Details**, vous devez voir que l'adresse source a été traduite en une adresse 209.165.x.x.