Chapitre 14	Sécuriser l'accès aux réseaux

1. Concepts de sécurité réseau

1.1 Qu'est-ce que la sécurité réseau ?

- À un niveau fondamental, la sécurité du réseau est l'opération qui consiste à protéger les données, les applications, les appareils et les systèmes qui sont connectés au réseau.
- Bien que la sécurité du réseau et la **cybersécurité** se chevauchent à bien des égards, la sécurité du réseau est le plus souvent définie comme un sous-ensemble de la cybersécurité.

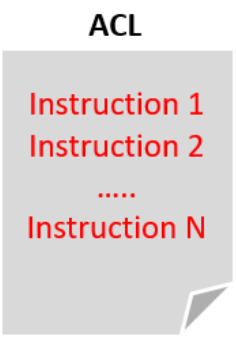
1.2 Quelques précautions élémentaires

- Pour bien protéger le reseau informatique interne il faut autoriser uniquement les services reseaux nécessaires aux traitements mis en place.
- Voici quelques précautions élémentaires qu'il faut prendre en consideration:
  - **Limiter les accès Internet** en bloquant les services non nécessaires (VoIP, pair à pair, etc.).
  - **Gérer les réseaux Wi-Fi.** Ils doivent utiliser un chiffrement à l'état de l'art (WPA2 ou WPA2-PSK avec un mot de passe complexe) et les réseaux ouverts aux invités doivent être séparés du réseau interne.
  - **Imposer un VPN pour l'accès à distance** ainsi que, si possible, une authentification forte de l'utilisateur (carte à puce, boitier générateur de mots de passe à usage unique (OTP), etc.).
  - **S'assurer qu'aucune interface d'administration n'est accessible directement depuis Internet.** La télémaintenance doit s'effectuer à travers un VPN.
  - **Limiter les flux réseau au strict nécessaire** en filtrant les flux entrants/sortants sur les équipements (pare-feu, proxy, serveurs, etc.) en utilisant les ACL et les techniques de filtrage.

2. Filtrage des paquets avec les ACL

2.1. Qu'est-ce qu'une ACL ?

- Une **ACL** (Access Control List en anglais et Liste de contrôle d'accès en français) est une série de commandes IOS qui déterminent si un routeur achemine ou abandonne les paquets en fonction des informations contenues dans l'en-tête de paquet.
- Les ACL font partie des fonctionnalités les plus utilisées du logiciel Cisco IOS.
- Une fois configurées, les ACL assurent les tâches suivantes :
  - Elles contrôlent le flux de trafic.
  - Elles filtrent le trafic en fonction de son type.



- Elles limitent le trafic réseau pour accroître les performances réseau.
- Elles fournissent un niveau de sécurité de base pour l'accès réseau.
- Etc.

2.2. Filtrage des paquets

- Le **filtrage des paquets** (ou filtrage statique des paquets) contrôle l'accès à un réseau en analysant les paquets entrants et sortants et en les transmettant ou en rejetant selon des critères spécifiques (adresse IP source, adresse IP de destination, …).
- Le filtrage des paquets intervient sur les couches 3 et 4 du modèle OSI.
- Les ACL contrôlent les paquets arrivant par les interfaces d'entrée, passant par le routeur et atteignant leur destination par les interfaces de sortie.

- Les ACL sont configurées pour s'appliquer au trafic entrant ou sortant. Elles ne gèrent pas les paquets provenant du routeur lui-même.
- Les **ACL entrantes** filtrent les paquets entrant dans une interface spécifique avant qu'ils soient acheminés vers l'interface de sortie.
- Les **ACL sortantes** filtrent les paquets après qu'ils ont été routés, et ce, quelle que soit l'interface de sortie.

2.3. Types des ACL IPv4

- Les ACL IPv4 peuvent être de type standard ou étendu :

ACL standard	Elle filtre les paquets IP en fonction de l'adresse source uniquement. La destination du paquet et les ports concernés ne sont pas évalués.
ACL étendue	Elle filtre les paquets en fonction de différents critères : type de protocole (ICMP, TCP, UDP, etc.), adresse IPv4 source et destination, ports TCP ou UDP source et destination, etc.

- Les ACL IPv4 peuvent être identifiées par un numéro ou un nom :

ACL IPv4 numérotée	Attribution d'un numéro à l'ACL (en fonction du protocole à filtrer) : - Plages 1 à 99 et 1300 à 1999 : ACL IPv4 standard - Pages 100 à 199 et 2000 à 2699 : ACL IPv4 étendue
ACL IPv4 nommée	Attribution d'un nom à l'ACL : - Les noms doivent se composer de caractères alphanumériques. - Il est conseillé d'écrire le nom en MAJUSCULES. - Les noms ne doivent pas contenir d'espaces ni de signes de ponctuation.

2.4. ACL IPv4 et masque générique

- Les ACL IPv4 incluent l'utilisation de masques génériques.
- Un **masque générique** est une chaîne de 32 chiffres binaires utilisés par le routeur pour déterminer quels bits de l'adresse à examiner afin d'établir une correspondance.
- Le masque générique se calcule comme étant l'inverse du masque de sous-réseau.
- Le mot **host** (hôte) peut remplacer le masque générique 0.0.0.0
- Le mot **any** (tous) peut remplacer le masque générique 255.255.255.255.

2.5. Procédure de configuration des ACL IPv4

- La procédure de configuration des ACL IPv4 (standard et étendue) suit les étapes suivantes :
  1. Créer de l'ACL (standard ou étendue)
  2. Appliquer l'ACL sur une interface (entrée ou sortie)
  3. Vérifier le fonctionnement de l'ACL

2.6. Configuration d'une ACL standard

- La commande de création d'une ACL IPv4 **standard numérotée** est la suivante :

Router(config)# **access-list** *number* { **deny** | **permit** | **remark** } *source* [*source-wildcard*]

number	Numéro de l'ACL. Il doit être compris entre 1 et 99 ou entre 1300 et 1999.
Deny	Refuse l'accès si les conditions sont respectées.
Permit	Autorise d'accès si les conditions sont respectées
Remark	Ajoute une remarque (commentaire) sur les instructions d'une ACL
Source	Numéro du réseau ou de l'hôte d'où provient le paquet.
Source-wildcard	Masque générique à appliquer à la source (facultatif).

- **Exemple** : créer dans une ACL 10 les instructions suivantes :
  - Une instruction qui refuse un hôte spécifique possédant l'adresse IP 192.168.10.10
  - Une instruction autorisant tout le réseau 192.168.10.0/24 en lui donnant une remarque.

```
R1(config)# access-list 10 permit host 192.168.10.10
R1(config)# access-list 10 remark Permit hosts from the 192.168.10.0 LAN
R1(config)# access-list 10 permit 192.168.10.0 0.0.0.255
```

- Remarque : Les entrées d'une ACL sont traitées de manière séquentielle. Par conséquent, **l'ordre dans lequel elles sont saisies est important.**
- Par exemple, dans l'ACL 4, l'instruction d'hôte peut toujours être configurée avant les instructions de plage.

```
R1(config)# access-list 4 permit host 192.168.10.10
R1(config)# access-list 4 deny 192.168.10.0 0.0.0.255
```

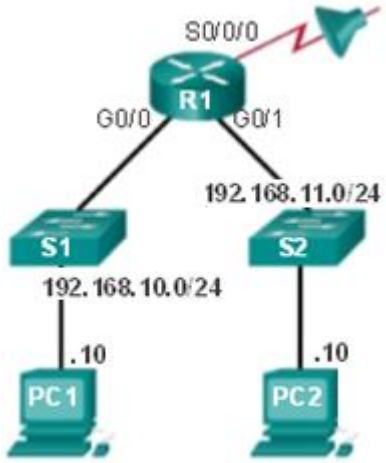
- Dans l'ACL 5 suivante, l'instruction d'hôte peut être configurée après l'instructions de plage si cela ne génère aucun conflit.

```
R1(config)# access-list 5 deny 192.168.10.0  0.0.0.255
R1(config)# access-list 5 permit host 192.168.11.10
```

- La commande pour appliquer une ACL standard aux interfaces est la suivante :

Appliquer une ACL standard à une interface	R1(config-if)# **ip access-group** {*acl-number* | *acl-name*} {**in** | **out**}
Désactiver l'ACL standard sur l'interface	R1(config-if)# **no ip access-group**

- Dans l'exemple, l'ACL créé permet de refuser un certain hôte et d'autoriser un sous-réseau spécifique

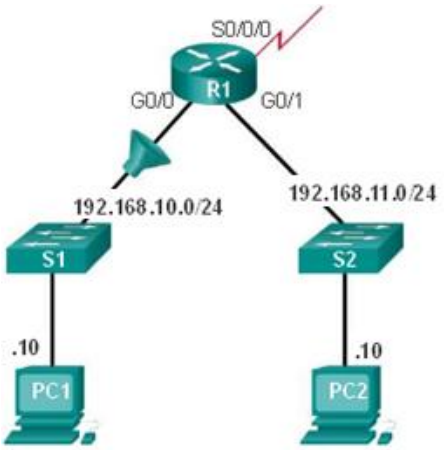



```
R1(config)# no access-list 1
R1(config)# access-list 1 remark Do not allow Guest workstation through
R1(config)# access-list 1 deny host 192.168.10.10
R1(config)#access-list 1 remark Allow devices from all other 192.168.X.X subnets
R1(config)# access-list 1 permit 192.168.10.0  0.0.0.255
R1(config)# interface s0/0/0
R1(config-if)# ip access-group 1 out
```

- Les commandes de création et d'application d'une ACL IPv4 standard nommée sont les suivantes :

Définir l'ACL standard nommée.	R(config)# **ip access-list standard** *nom*
Spécifier les permissions ou les rejets.	R(config-std-nacl)# {**permit** | **deny** | **remark**} *source* [*masque*]
Appliquer l'ACL nommée à une interface.	R(config-if)# **ip access-group** *nom* [**in** | **out**]

- Exemple de création et d'application d'une ACL standard nommée :




```
R1(config)# ip access-list standard NO_ACCESS
R1(config-std-nacl)# remark Do not allow access from Lab workstation
R1(config-std-nacl)# remark Allow access from all other networks
R1(config-std-nacl)# deny host 192.168.11.10
R1(config-std-nacl)# permit any
R1(config-std-nacl)# exit
R1(config)# interface g0/0
R1(config-if)# ip access-group NO_ACCESS out
```

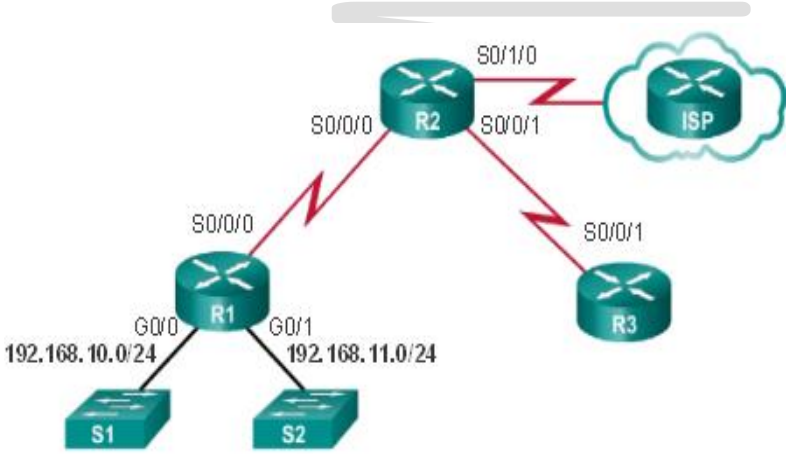
2.7. Configuration d'une ACL IPv4 étendue

- La commande de création d'une ACL IPv4 **étendue numérotée** est la suivante :

access-list *num* {**deny**|**permit**|**remark**} *prt src* [*mask_src*][*oper*][*port*] *des* [*mask_des*][*oper*][*port*] [**established**]

num	Numéro de l'ACL étendue.
prt	Protocole = Nom ou numéro d'un protocole Internet (icmp, ip, tcp ou udp)
src	Source = numéro du réseau ou de l'hôte d'où provient le paquet.
des	Destination = numéro du réseau ou de l'hôte auquel le paquet est envoyé.
Mas_gen_src	Masque générique appliqué à la source (facultatif).
Mas_gen_dst	Masque générique appliqué à la destination (facultatif).
port	Numéro décimal ou nom d'un port TCP ou UDP.
opr	Opérateur = compare les ports de source ou de destination (facultatif) : lt (=inférieur à), Gt (=supérieur à), Eq (=égal à), Neq (=non égal à) et Range (=plage inclusive).
established	Pour le protocole TCP uniquement : indique une connexion établie (facultatif).

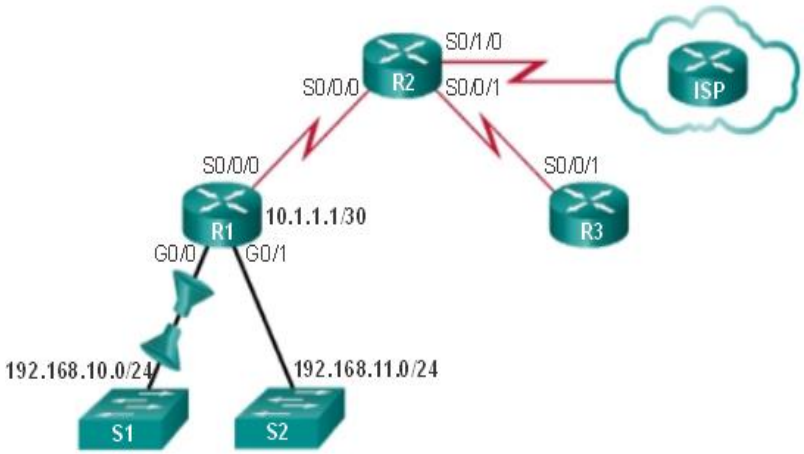
- Dans l'exemple suivant, L'ACL 103 autorise le trafic en provenance de toute adresse sur le réseau 192.168.10.0 à accéder à n'importe quelle destination, à condition que le trafic soit transféré via les ports 80 (HTTP) et 443 (HTTPS) uniquement. L'ACL 104 bloque tout trafic entrant, à l'exception des connexions établies précédemment (HTTP et HTTPS).



R(config)# **access-list 103 permit tcp 192.168.10.0 0.0.0.255 any eq 80**
R(config)# **access-list 103 permit tcp 192.168.10.0 0.0.0.255 any eq 443**
R(config)# **access-list 104 permit tcp any 192.168.10.0 0.0.0.255 established**

- L'application d'une ACL IPv4 étendue numérotée aux interfaces se fait par la commande suivante. Les ACL étendues doivent généralement être appliquées près de la source.

R(config-if)# **ip access-group** *num-acl* [in|out]



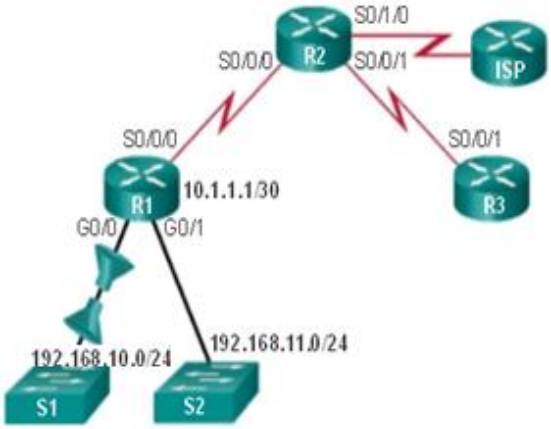
R1(config)# **int g0/0**
R1(config-if)# **ip access-group 103 in**
R1(config-if)# **ip access-group 104 out**

Etant donné que G0/0 est l'interface la plus proche de la source du trafic cible.

- La création et l'application d'une ACL IPv4 étendue nommée se fait par les commandes suivantes :

Définir l'ACL standard nommée.	R(config)# **ip access-list extended** *nom*
Spécifier les permissions ou les rejets.	R(config-ext-nacl)# {**permit** | **deny** | **remark**} *instruction*
Appliquer l'ACL nommée à une interface.	R(config-if)# **ip access-group** *nom* {**in** | **out**}

- Voici un exemple de création et d'application de deux ACL IPv4 étendue nommée :



R1(config)#**ip access-list extended SURFING**
R1(config-ext-nacl)#**permit tcp 192.168.10.0 0.0.0.255 any eq 80**
R1(config-ext-nacl)#**permit tcp 192.168.10.0 0.0.0.255 any eq 443**

R1(config)#**ip access-list extended BROWSING**
R1(config-ext-nacl)#**permit tcp any 192.168.10.0 0.0.0.255 established**

R1(config)#**interface g0/0**
R1(config-if)#**ip access-group SURFING in**
R1(config-if)#**ip access-group BROWSING out**

2.8. Commandes de diagnostic des ACL IPv4

Afficher toutes les ACL configurées.	R1# **show access-lists**
Afficher la configuration d'une ACL numérotée ou nommée.	R1# **show access-lists** [*num* | *nom*]
Vérifier les ACL appliquées sur une interface.	R1# **show ip interface** *interface*
Supprimer une ACL IPv4 numérotée (standard ou étendue)	R(config)#**no access-list** *num*
Supprimer une ACL IPv4 nommée (standard ou étendue).	R(config)#**no ip access-list** [**standard** | **extended**] *nom*
Désactiver une ACL IPv4 numérotée sur une interface.	R(config-if)#**no access-group** *num* [**in** | **out**]

2.9. Configuration des ACL IPv6

- Les ACL IPv6 sont **nommées** uniquement (pas d'ACL IPv6 numérotées)
- La fonctionnalité d'une ACL IPv6 est équivalente à celle d'une ACL IPv4 étendue.
- **Remarque** : une liste de contrôle d'accès IPv4 et une liste de contrôle d'accès IPv6 ne peuvent pas porter le même nom.
- Voici une comparaison entre les ACL IPv4 et les ACL IPv6 :

ACL IPv4	ACL IPv6
L'application de l'ACL aux interfaces se fait via la commande **ip access-group**.	L'application de l'ACL aux interfaces se fait par la commande **ipv6 traffic-filter**.
Utilisation de masque générique.	Utilisation de longueur de préfixe.
Les instructions implicites sont **deny any** et **deny any any**	Les instructions implicites sont **permit icmp any any nd-na** et **permit icmp any any nd-ns**. **nd-na** = découverte de voisin-annonce de voisin. **nd-ns** = découverte de voisin-sollicitation de voisin.

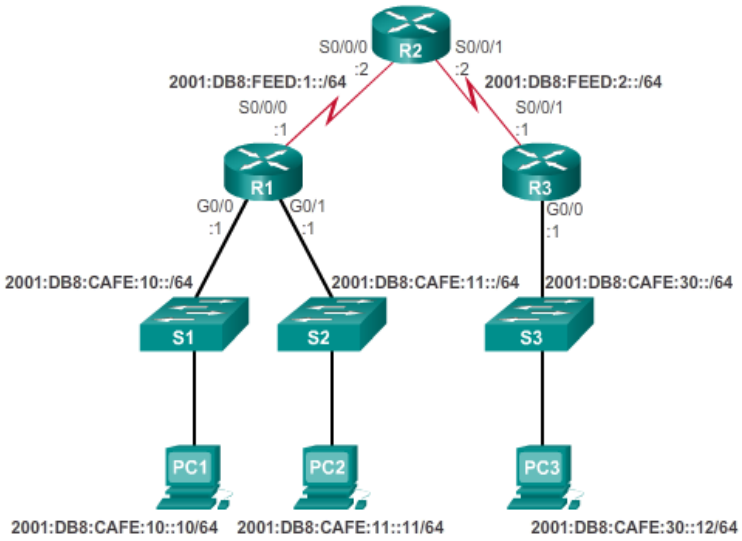
- La configuration d'une ACL IPv6 est similaire à celle d'une liste de contrôle d'accès étendue IPv4 nommée.

  Voici les commandes de création et d'application d'une ACL IPv6 sont les suivantes :

```
R1(config)# ipv6 access-list access-list-name
R1(config-ipv6-acl)# deny | permit protocol {source-ipv6-
prefix/prefix-length | any | host source-ipv6-address} [operator
[port-number]] {destination-ipv6-prefix/prefix-length | any | host
destination-ipv6-address} [operator [port-number]]
```

deny | **permit**	Indique si le paquet doit être refusé ou autorisé.
protocol	Nom ou numéro du protocole correspondant.
Source-ipv6-prefix/prefix-length *Destination-ipv6-address*	Réseau source ou de destination IPv6.
any	Correspond à toutes les adresse (il sert d'abréviation du préfixe IPv6 ::/0)
host	Après ce mot, on saisit l'adresse source ou de destination de l'hôte IPv6 pour lequel on définit les conditions de refus ou d'autorisation.
operator	(Facultatif) Opérande comparant les ports source ou de destination du protocole spécifié. Les opérandes sont **it** (inférieur à), **gt** (supérieur à) ; **eq** (égal à), **neq** (non égal à) et **range** (plage).
port-number	(Facultatif) nombre décimal ou nom d'un port TCP ou UDP de filtrage de TCP ou UDP respectivement.

- Dans l'exemple suivant, R1 est configuré avec une ACL IPv6 pour refuser le trafic FTP vers 2001:DB8:CAFE:11::/64. Les ports 20 (données FTP) et 21 (contrôle FTP) doivent être bloqués. Le filtre doit être appliqué en entrée sur G0/0 de R1 pour refuser uniquement le trafic provenant du réseau 2001:DB8:CAFE:10::/64




```
R1 (config)# ipv6 access-list NO-FTP-TO.11
R1 (config-ipv6-acl)# deny tcp any 2001:db8:cafe:11::/64 eq ftp
R1 (config-ipv6-acl)# deny tcp any 2001:db8:cafe:11::/64 eq ftp-data
R1 (config-ipv6-acl)# permit ipv6 any any
```

```
R1 (config)# int g0/0
R1 (config-if)# ipv6 traffic-filter NO-FTP-TO-11 in
```

3. Accès au réseau public avec NAT

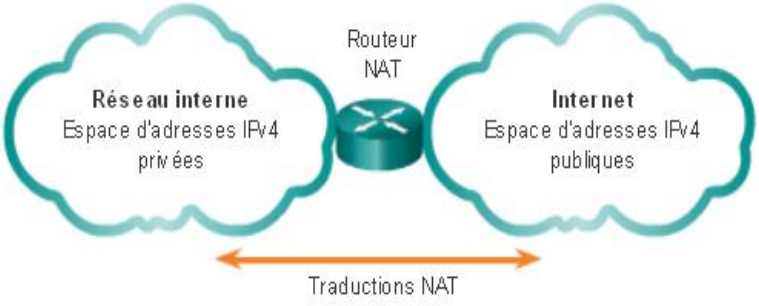
3.1. Rappel sur les adresses IP privées

- Il n'existe pas suffisamment d'adresses IPv4 publiques pour pouvoir attribuer une adresse unique à chaque périphérique connecté à Internet.
- Les réseaux sont généralement mis en œuvre à l'aide d'adresses IPv4 privées (RFC 1918) :

Classe	Plage d'adresses internes RFC 1918	Préfixe CIDR
A	10.0.0.0 – 10.255.255.255	10.0.0.0/8
B	172.16.0.0 – 172.31.255.255	172.16.0.0/12
C	192.168.0.0 – 192.168.255.255	192.168.0.0/16

- Les adresses privées sont utilisées au sein d'un réseau pour permettre aux périphériques de communiquer localement. Ces adresses privées ne peuvent pas être acheminées sur Internet (**adresses non routables**).

3.2. NAT, c'est quoi ?



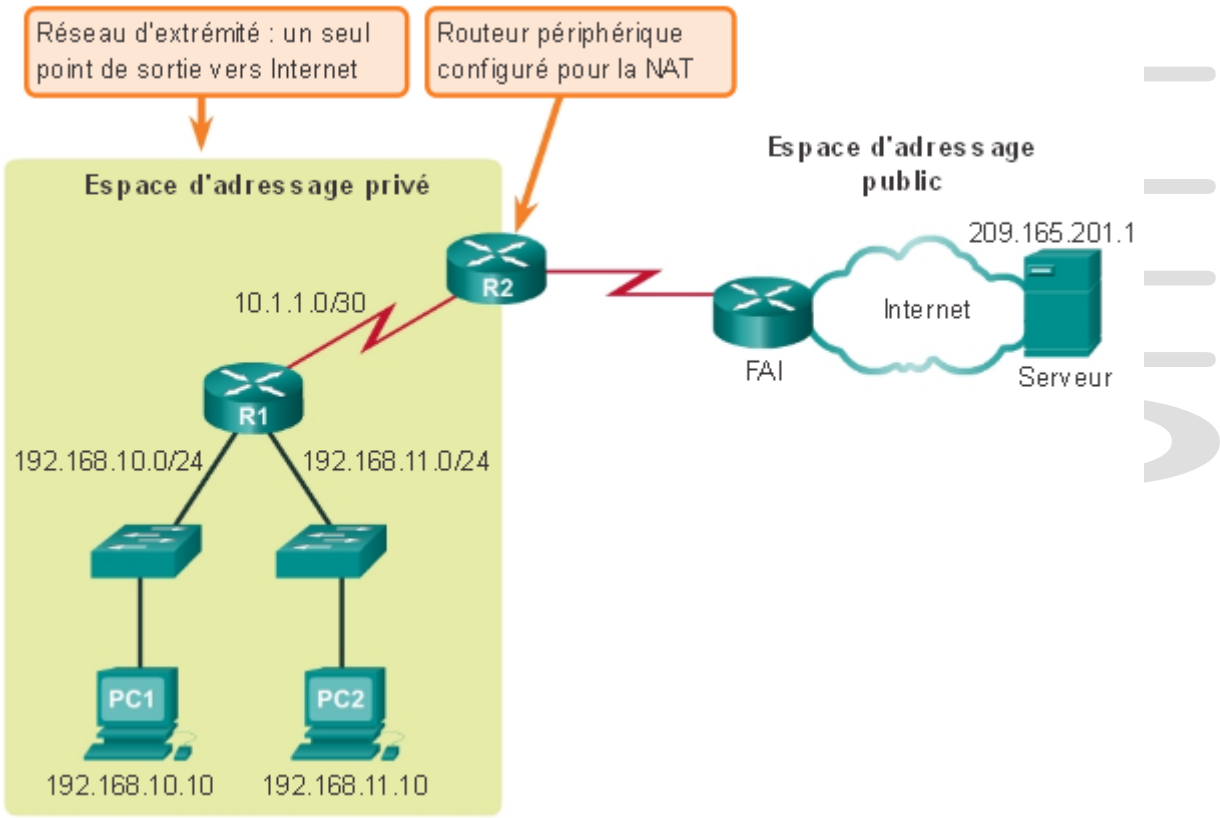
- **NAT** (Network Address Translation pour Traduction d'adresse réseau en français) assure la traduction des adresses privées en adresses publiques.
- La NAT permet à un périphérique possédant une adresse IPv4 privée d'accéder aux ressources situées en dehors de son réseau privé, notamment celles d'Internet.

- Parmi les avantages de NAT, on peut citer :
  - *Préserver les adresses IPv4 privées* : une seule et même adresse IPv4 publique peut être partagée par des centaines d'équipements, chacun étant configuré avec une adresse IPv4 privée unique. Sans la NAT, l'espace d'adressage IPv4 aurait été saturé bien avant l'an 2000.
  - *Ajouter un niveau de confidentialité et de sécurité à un réseau* : NAT empêche les réseaux externes de voir les adresses IPv4 internes.
- Il existe trois types de NAT :

NAT statique	Mappage un à un entre les adresses locale et globale.
NAT dynamique	Mappage de plusieurs adresses locales et globales.
PAT	Mappage de plusieurs adresses locales et globales vers une seule.

3.3. Terminologie NAT

- **Routeur NAT** (routeur configuré pour la NAT) peut être configuré avec une ou plusieurs adresses IPv4 publiques valides (appelées **pool NAT**).
- Lorsqu'un périphérique interne envoie du trafic hors du réseau, le routeur NAT traduit l'adresse IPv4 interne du périphérique en une adresse publique du pool NAT. Pour les périphériques externes, tout le trafic entrant sur le réseau et sortant de celui-ci semble posséder une adresse IPv4 publique du pool d'adresses fourni.



- Un routeur NAT fonctionne généralement à la périphérie d'un **réseau d'extrémité** (un réseau ayant une seule connexion à son réseau voisin, avec un seul chemin pour émettre et recevoir).
- **Réseau interne** est un ensemble des réseaux soumis à la traduction NAT.
- **Réseau externe** est tout autre réseau non interne.

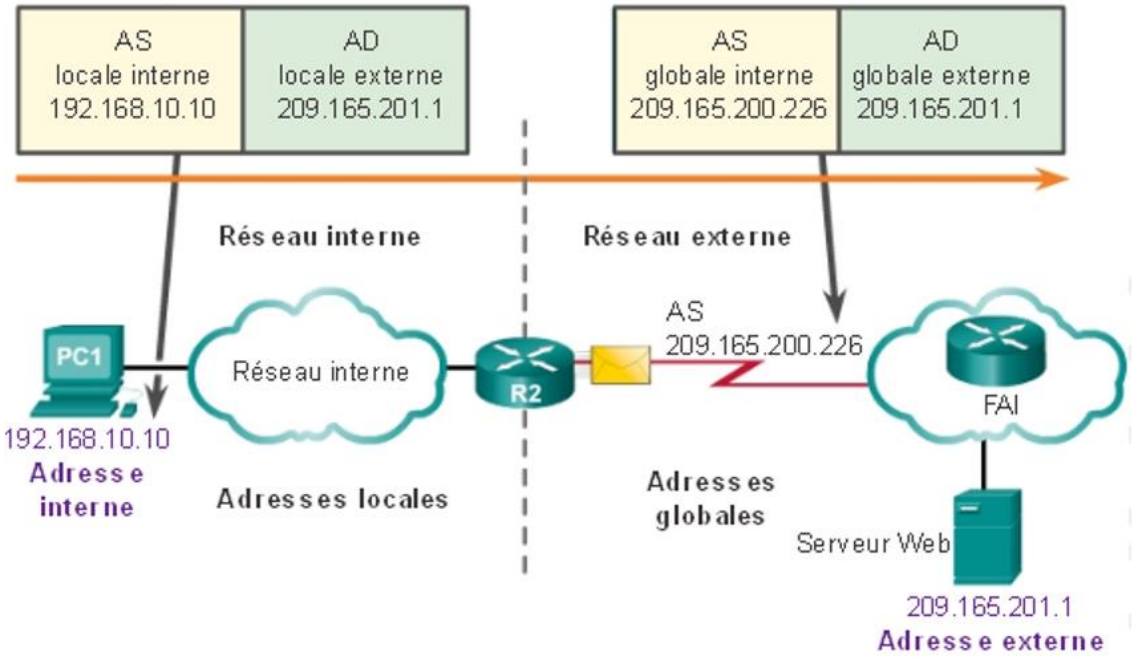
3.4. Types d'adresses NAT

- La fonction NAT comprend quatre types d'adresses :

Adresse interne	Adresse du périphérique traduite via la NAT.
Adresse externe	Adresse du périphérique de destination.
Adresse locale	Elle correspond à toute adresse qui apparaît sur la partie interne du réseau.
Adresse globale	Elle correspond à toute adresse qui apparaît sur la partie externe du réseau.

- **Remarque :** Pour déterminer le type d'adresse utilisé, il est important de retenir que la terminologie NAT est toujours appliquée du point de vue du périphérique dont l'adresse est traduite :

- **Exemple :** PC1 possède l'@ locale interne 192.168.10.10. Du point de vue de PC1, le serveur Web possède l'@ externe 209.165.201.1. Lorsque des paquets sont envoyés de PC1 à l'@ globale du serveur Web, l'@ locale interne de PC1 est traduite en 209.165.200.226 (@ globale interne). L'@ du périphérique externe n'est généralement pas traduite, car il s'agit en principe d'une @IPv4 publique. PC1 possède des adresses locale et globale différentes, tandis que le serveur Web possède la même adresse IPv4 publique pour les deux. Du point de vue du serveur Web, le trafic en provenance de PC1 semble provenir de 209.165.200.226 (= @ globale interne).



3.5. NAT statique

- **NAT statique** est un mappage de type un à un des adresses locales et globales. Ces mappages statiques sont configurés par l'administrateur réseau et restent constants.
- Exemple **:** R2 est configuré avec des mappages statiques pour les adresses locales internes de Svr1, PC2 et PC3. Lorsque ces périphériques envoient du trafic vers Internet, leurs adresses locales internes sont traduites en adresses globales internes (celles configurées). Pour les réseaux externes, ces périphériques possèdent des adresses IPv4 publiques.

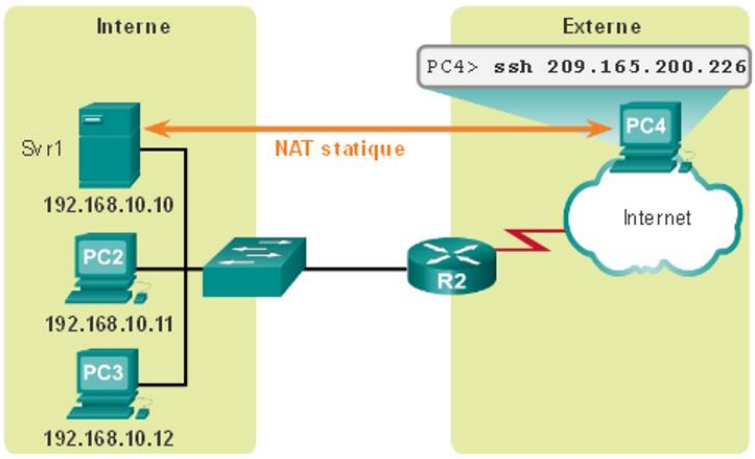


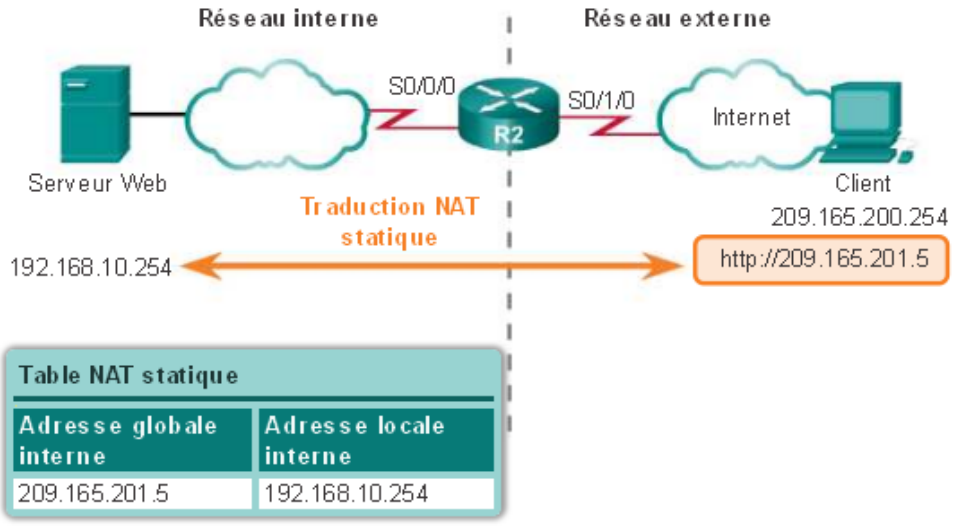
Table NAT statique	
Adresse locale interne	**Adresse globale interne (Adresses accessibles via R2)**
192.168.10.10	209.165.200.226
192.168.10.11	209.165.200.227
192.168.10.12	209.165.200.228

- La NAT statique est particulièrement utile pour les serveurs Web ou les périphériques qui doivent posséder une adresse permanente accessible depuis Internet, notamment les serveurs Web d'entreprise. Elle sert également aux périphériques qui doivent être accessibles à distance par le personnel autorisé (dans l'exemple, un administrateur réseau utilisant PC4 peut établir une connexion SSH à l'adresse globale interne de Svr1 qui est 209.165.200.226).
- La NAT statique nécessite qu'il existe suffisamment d'adresses publiques disponibles pour satisfaire le nombre total de sessions utilisateur simultanées.
- La procédure de configuration de NAT statique est la suivante :

1. Etablir la traduction statique entre une adresse locale interne et une adresse globale interne.	R(config)# **ip nat inside source static** *local-ip global-ip*
2. Spécifier l'interface interne et la signaler comme connectée à l'intérieur.	R(config)# **interface** *type number* R(config-if)# **ip nat inside**
3. Spécifier l'interface externe et la signaler comme connectée avec l'extérieur.	R(config)# **interface** *type number* R(config-if)# **ip nat outside**

- Dans l'exemple suivant, R2 est configuré avec la NAT statique pour permettre aux périphériques sur le réseau Internet d'accéder au serveur Web. Le client situé sur le réseau externe accède au serveur Web à l'aide d'une

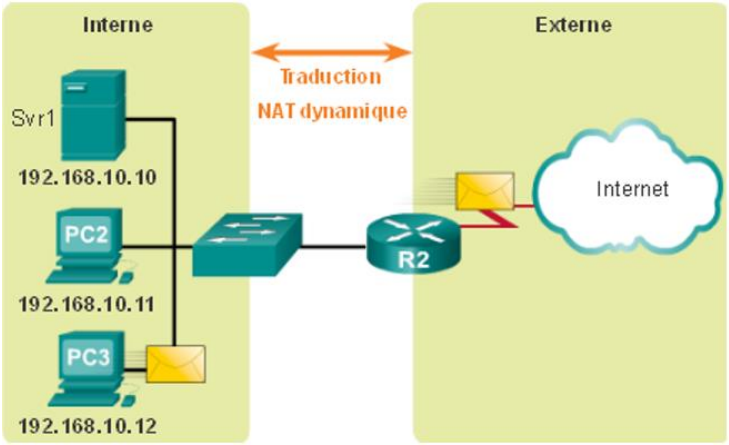
adresse IPv4 publique (209.165.201.5). La NAT statique traduit l'adresse IPv4 publique en adresse IPv4 privée.




```
R2(config)# ip nat inside source static 192.168.10.254 209.165.201.5
R2(config)# interface S0/0/0
R2(config-if)# ip nat inside
R2(config-if)# exit
R2(config)# interface S0/1/0
R2(config-if)# ip nat outside
```

3.6. NAT dynamique

- La NAT dynamique utilise un pool d'adresses publiques et les attribue selon la méthode du premier arrivé, premier servi (*FIFO = First In is the First Out*).
- Lorsqu'un périphérique interne demande l'accès à un réseau externe, la NAT dynamique attribue une adresse IPv4 publique disponible du pool.
- Dans l'exemple suivant, PC3 a accédé à Internet à l'aide de la première adresse disponible dans le pool NAT dynamique (209.165.200.226). Les autres adresses sont toujours disponibles.

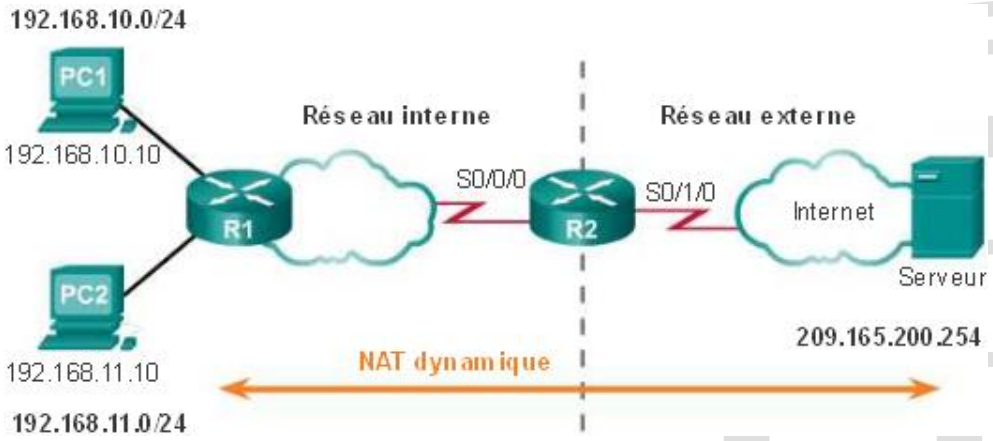


Pool NAT IPv4	
Adresse locale interne	**Pool d'adresse globale internes (Adresses accessibles via R2)**
192.168.10.12	209.165.200.226
Disponible	209.165.200.227
Disponible	209.165.200.228
Disponible	209.165.200.229
Disponible	209.165.200.230

- Remarque : Comme la fonction NAT statique, la NAT dynamique nécessite qu'il existe suffisamment d'adresses publiques disponibles pour satisfaire le nombre total de sessions utilisateur simultanées.
- La procédure de configuration de NAT dynamique est la suivante :

1. Définir un pool d'adresses globales à utiliser pour la traduction.	R(config)# **ip nat pool** *name start-ip end-ip* {**netmask** *netmask* | **prefix-length** *prefix-length*}
2. Configurer une ACL standard autorisant les adresses qui doivent être traduites.	R(config)# **access-list** *acl-number* **permit** *source [source-wildcard]*
3. Etablir une traduction dynamique de la source, en spécifiant la liste d'accès et le pool définis lors des étapes précédentes.	R(config)# **ip nat inside source list** *acl-number* **pool** *name*
4. Identifier l'interface interne.	R(config)# **interface** *type number* R(config-if)# **ip nat inside**
5. Identifier l'interface externe.	R(config)# **interface** *type number* R(config-if)# **ip nat outside**

- Voici un exemple de configuration de NAT dynamique :




```
R2(config)# ip nat pool NAT-POOL1 209.165.200.226 209.165.200.240 netmask 255.255.255.224
R2(config)# access-list 1 permit 192.168.0.0 0.0.255.255
R2(config)# ip nat inside source list 1 pool NAT-POOL1
R2(config)# interface S0/0/0
R2(config-if)# ip nat inside
R2(config-if)# exit
R2(config)# interface S0/1/0
R2(config-if)# ip nat outside
```

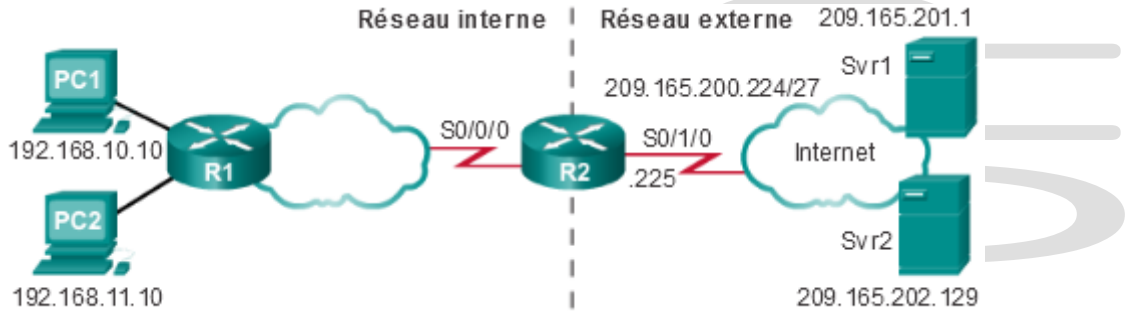
3.7. PAT

- La **PAT** (Port Address Translation pour Traduction d'adresse de port) est également appelée **surcharge NAT**.
- La PAT mappe plusieurs adresses IPv4 privées à une seule adresse IPv4 publique unique ou à quelques adresses.

- PAT est la forme la plus courante de NAT.
- PAT est la plus utilisée sur la plupart des routeurs de particuliers : Le FAI attribue une adresse au routeur, mais plusieurs membres de la famille peuvent accéder simultanément à Internet.
- Chaque adresse privée est également identifiée par un numéro de port. Lorsqu'un périphérique établit une session TCP/IP, il génère une valeur de port source TCP ou UDP pour identifier de manière unique la session. Lorsque le routeur NAT reçoit un paquet du client, il utilise son numéro de port source pour identifier de manière unique la traduction NAT spécifique.
- Si un site a obtenu plusieurs adresses IPv4 publiques, celles-ci peuvent faire partie d'un pool utilisé par la PAT. Cela équivaut à la NAT dynamique, sauf qu'il n'y a pas suffisamment d'adresses publiques pour permettre un mappage de type un à un des adresses internes/externes.
- La procédure de configuration de la **PAT avec un pool d'adresses** est la suivante :

1. Définir un pool d'adresses globales à utiliser pour la traduction de surcharge.	R(config)# **ip nat pool** *name start-ip end-ip* {**netmask** *netmask* | **prefix-length** *prefix-length*}
2. Définir une ACL standard autorisant les adresses qui doivent etre traduites.	R(config)# **access-list** *acl-number* **permit** *source [source-wildcard]*
3. Etablir la traduction de surcharge, en spécifiant la liste d'accès et le pool définis précédemment.	R(config)# **ip nat inside source list** *acl-number* **pool** *name* **overload**
4. Identifier l'interface interne.	R(config)# **interface** *type number* R(config-if)# **ip nat inside**
5. Identifier l'interface externe.	R(config)# **interface** *type number* R(config-if)# **ip nat outside**

- Voici un exemple de configuration de PAT pour un pool d'adresses :




```
R2(config)# ip nat pool NAT-POOL2 209.165.200.226 209.165.200.240 netmask 255.255.255.224
R2(config)# access-list 1 permit 192.168.0.0 0.0.255.255
R2(config)# ip nat inside source list 1 pool NAT-POOL2 overload
R2(config)# interface S0/0/0
R2(config-if)# ip nat inside
```

```
R2(config-if)# exit
R2(config)# interface S0/1/0
R2(config-if)# ip nat outside
```

- Il est ainsi possible de configurer la PAT avec une seule adresse publique. Voici la procédure à suivre :

1. Définir une ACL standard autorisant les adresses qui doivent être traduites.	R(config)# **access-list** *acl-number* **permit** *source [source-wildcard]*
2. Etablir la traduction de surcharge, en spécifiant l'ACL, l'interface de sortie et les options de surcharge.	R(config)# **ip nat inside source list** *acl-number* **interface** *type number* **overload**
3. Identifier l'interface interne.	R(config)# **interface** *type number* R(config-if)# **ip nat inside**
4. Identifier l'interface externe.	R(config)# **interface** *type number* R(config-if)# **ip nat outside**

- Dans l'exemple suivant, les adresses de tous les hôtes du réseau 192.168.0.0/16 (correspondant à l'ACL 1) qui envoient du trafic via le routeur R2 sur Internet sont traduites en l'adresse IPv4 209.165.200.225 (adresse IPv4 de l'interface S0/1/0). Les flux de trafic sont identifiés par les numéros de port dans la table NAT, car le mot-clé **overload** a été utilisé.

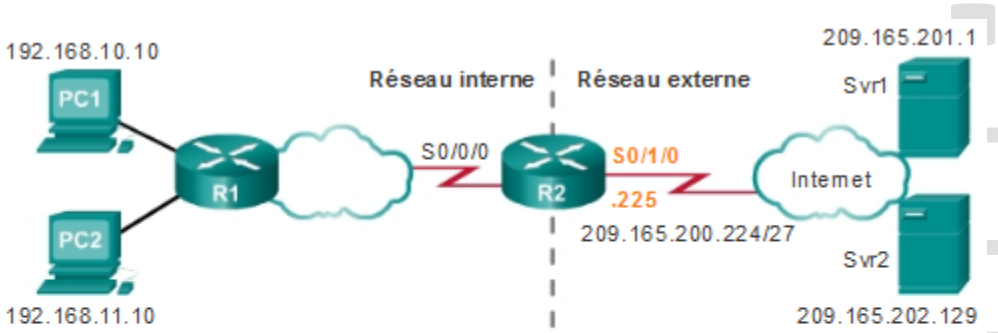


Table NAT

Adresse globale interne	Adresse locale interne	Adresse locale externe	Adresse globale externe
209.165.200.225:1444	192.168.10.10:1444	209.165.201.1:80	209.165.201.1:80
209.165.200.225:1445	192.168.10.11:1444	209.165.202.129:80	209.165.202.129:80

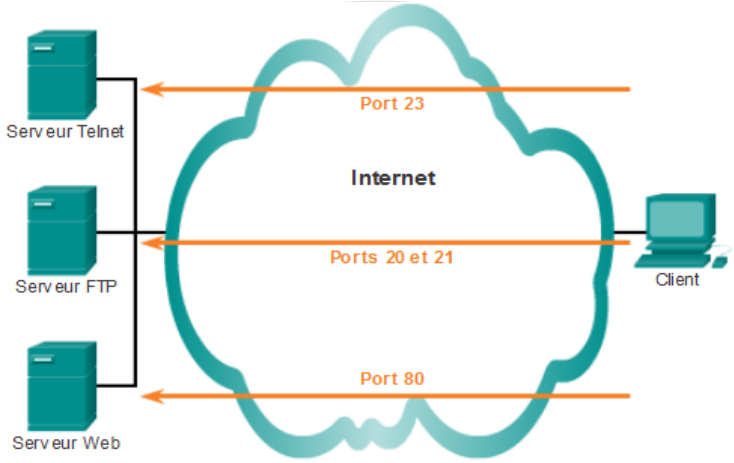
```
R2(config)# access-list 1 permit 192.168.0.0 0.0.255.255
R2(config)# ip nat inside source list 1 interface S0/1/0 overload
R2(config)# interface S0/0/0
R2(config-if)# ip nat inside
R2(config-if)# exit
R2(config)# interface S0/1/0
R2(config-if)# ip nat outside
```

3.8. Vérification de la traduction d'adresse réseau

show ip nat translations	Affiche toutes les traductions NAT configurées et créées par le trafic.
show ip nat translations verbose	Affiche des informations supplémentaires sur chaque traduction, notamment la date de création et la durée d'utilisation d'une entrée.
show ip nat statistics	Affiche des informations sur le nombre total de traduction actives, les paramètres de configuration NAT, le nombre d'adresses dans le pool et le nombre d'adresses attribuées.
show running-config	Affiche les valeurs correspondantes aux commandes NAT, interface et pool.
clear ip nat statistics	Efface les statistiques des transactions NAT.

3.9. Redirection de port

- La **redirection de port** (parfois appelée **tunneling**) consiste à transférer le trafic adressé à un port réseau spécifique d'un nœud réseau à un autre.
- Cette technique permet à un utilisateur externe d'atteindre un port sur une adresse IPv4 privée (dans un réseau local) à partir de l'extérieur, via un routeur configuré pour la NAT.
- Exemple : les services Web et le FTP sortant, exigent que les ports du routeur soient redirigés ou ouverts pour que ces applications puissent fonctionner. La NAT masquant les adresses internes, l'opération peer to peer ne fonctionne que de l'intérieur vers l'extérieur, car la NAT peut mapper les requêtes sortantes avec les réponses entrantes.
- Le problème est que la NAT n'autorise pas les requêtes provenant de l'extérieur. Ce problème peut être résolu par une intervention manuelle. La redirection de port peut être configurée pour identifier des ports spécifiques pouvant être redirigés vers des hôtes internes.



- Les applications logicielles Internet interagissent avec des ports utilisateur qui doivent être ouverts ou à la disposition de ces applications. Les applications utilisent des ports différents. Cela permet aux applications et aux routeurs d'identifier les services réseau de manière prévisible. Par exemple, HTTP fonctionne sur le port réservé 80. Lorsque quelqu'un saisit l'adresse **http://cisco.com**, le navigateur affiche le site Web de Cisco Systems, Inc. Notez qu'il n'est pas nécessaire de préciser le numéro de

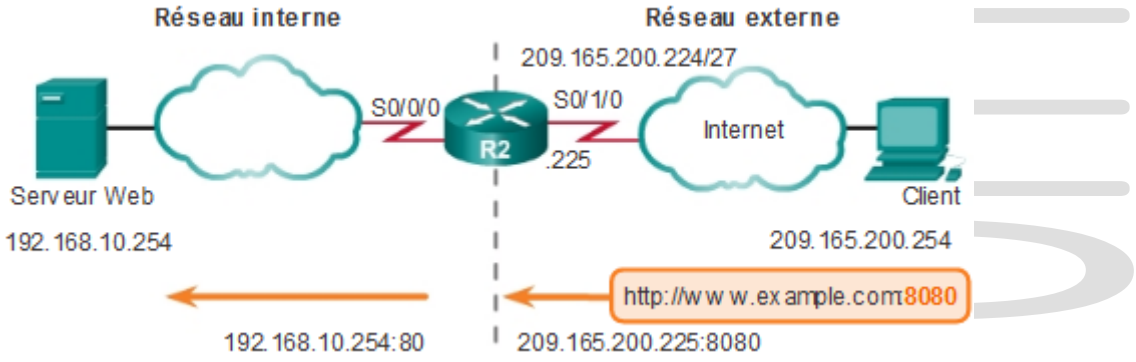
port HTTP pour demander la page, car l'application suppose qu'il s'agit du port 80. Si un autre numéro de port est requis, il peut être ajouté à la fin de l'URL après le signe deux-points (:). Par exemple, si le serveur Web de Cisco écoute le port 8080, l'utilisateur saisit **http://www.cisco.com:8080**.

- La redirection correspond à la traduction NAT statique avec un numéro de port TCP ou UDP spécifique.

```
ip nat inside source {static {tcp | udp local-ip local-port
global-ip global-port} [extendable]
```

Paramètre	Description
`tcp` ou `udp`	Indique s'il s'agit d'un numéro de port TCP ou UDP.
`local-ip`	Adresse IPv4 attribuée à l'hôte sur le réseau interne, généralement à partir de l'espace d'adressage privé de RFC 1918.
`local-port`	Définit le port TCP/UDP local dans une plage de 1 à 65 535. Il s'agit du numéro de port que le serveur écoute.
`global-ip`	Adresse IPv4 unique au monde d'un hôte interne. Il s'agit de l'adresse IP que les clients externes utiliseront pour atteindre le serveur interne.
`global-port`	Définit le port TCP/UDP global dans une plage de 1 à 65 535. Il s'agit du numéro de port que le client externe utilisera pour atteindre le serveur interne.
`extendable`	L'option `extendable` est appliquée automatiquement. Le mot-clé `extendable` permet à l'utilisateur de configurer plusieurs traductions statiques ambiguës (les traductions ambiguës sont des traductions possédant la même adresse locale ou globale). Il permet au routeur d'étendre la traduction à plusieurs ports si nécessaire.

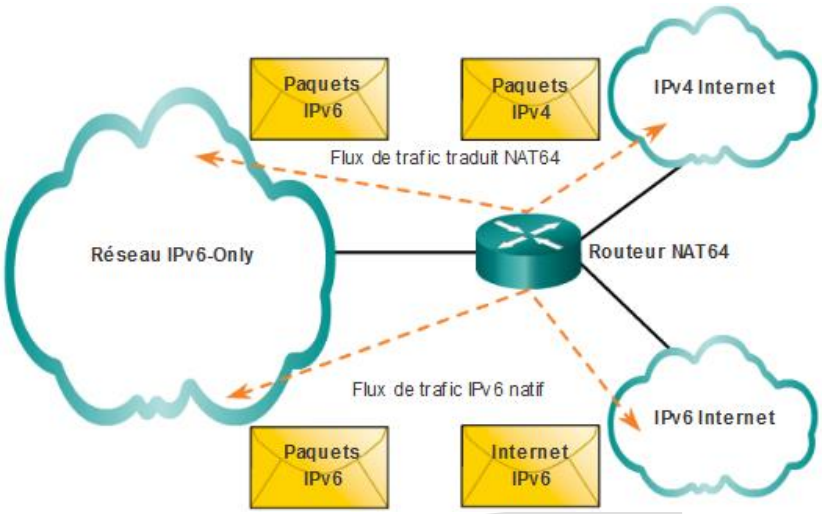
- Voici un exemple de configuration de la redirection




```
R2(config)# ip nat inside source static tcp 192.168.10.254 80 209.165.200.255 8080
R2(config)# interface S0/0/0
R2(config-if)# ip nat inside
R2(config-if)# exit
R2(config)# interface S0/1/0
R2(config-if)# ip nat outside
```

3.10. NAT pour IPv6

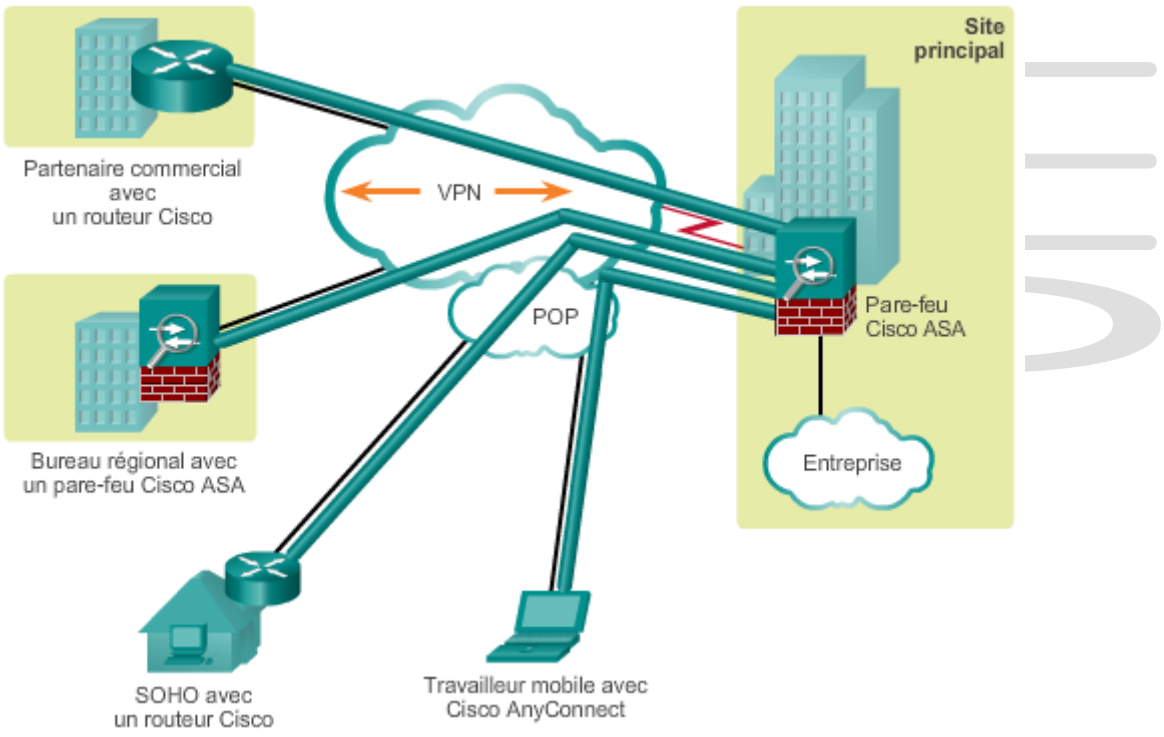
- La NAT pour IPv6 est utilisée dans un contexte très différent de la NAT pour IPv4.
- Les différentes NAT pour IPv6 servent à fournir de façon transparente un accès entre les réseaux IPv6-only et les réseaux ipv4-only (appelées **NAT64**).
- NAT pour IPv6 ne sert pas à traduire des adresses IPv6 privées en adresses IPv6 globales.



4. Concepts VPN

4.1. Définition de VPN

- La sécurité est un problème lorsque les entreprises utilisent le réseau Internet public pour mener à bien leurs activités.
- La figure suivante illustre les topologies utilisées par les réseaux modernes pour connecter des emplacements distants. Dans certains cas, les sites distants sont uniquement connectés au siège, alors que dans d'autres cas, ils sont connectés à divers sites.



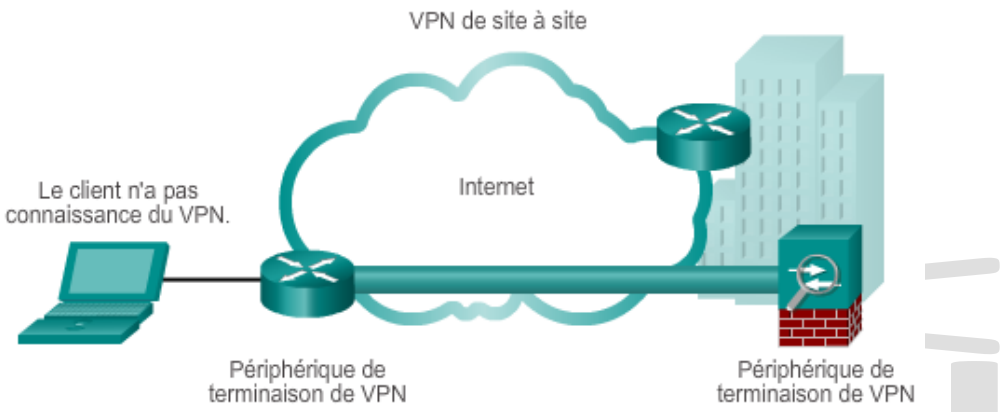
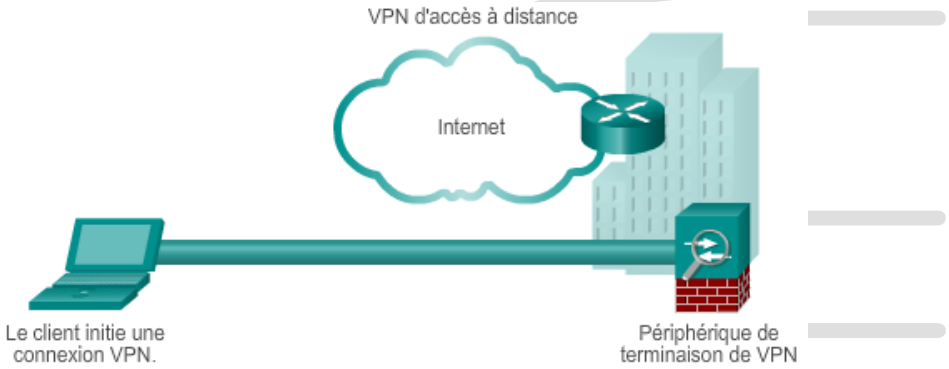
- Les entreprises utilisent des **VPN** (Virtual Private Network) pour créer une connexion sécurisée de bout en bout sur le réseau Internet.
- Un VPN sert à créer un tunnel privé sur un réseau public. Les données peuvent être sécurisées à l'aide des protocoles du chiffrement, tel que IPSec.
- Un VPN est un réseau privé créé par tunneling sur un réseau public, généralement Internet. Un VPN est un environnement de communication dans lequel l'accès est strictement contrôlé de manière à autoriser les connexions homologues au sein d'une communauté définie d'intérêt.
- Une passerelle VPN est requise pour l'implémentation de VPN. La passerelle VPN peut être un routeur, un pare-feu ou un périphérique Cisco ASA.

4.2. Avantages des VPN

Réductions des coûts	Les VPN permettent aux entreprises d'utiliser un transport Internet tiers et économique pour la connexion des bureaux et des utilisateurs distants au site principal, éliminant par conséquent le besoin de disposer de liaisons WAN onéreux.
Évolutivité	Les VPN permettent aux entreprises d'utiliser l'infrastructure d'Internet des FAI et des périphériques, ce qui permet d'ajouter facilement de nouveaux utilisateurs.
Compatibilité avec la technologie haut débit	Les VPN permettent aux travailleurs mobiles de bénéficier d'une connectivité haut débit rapide, comme la technologie DSL, pour accéder au réseau de leur entreprise.
Sécurité	Les VPN peuvent inclure des mécanismes de sécurité offrant un niveau de sécurité très élevé grâce à l'utilisation de protocoles de chiffrement et d'authentification.

4.3. Types des VPN

VPN site à site	- Un VPN de site à site est créé lorsque les périphériques situés des deux côtés de la connexion VPN connaissent par avance la configuration VPN. - Le VPN reste statique et les hôtes internes ne savent pas qu'un VPN existe. - Dans un VPN de site à site, les hôtes finaux envoient et reçoivent le trafic TCP/IP normal par l'intermédiaire d'une passerelle VPN. - Un VPN site à site est une extension d'un réseau étendu classique. - Les VPN site à site connectent entre eux des réseaux entiers. Ils peuvent par exemple connecter un réseau de filiale au réseau du siège d'une entreprise.

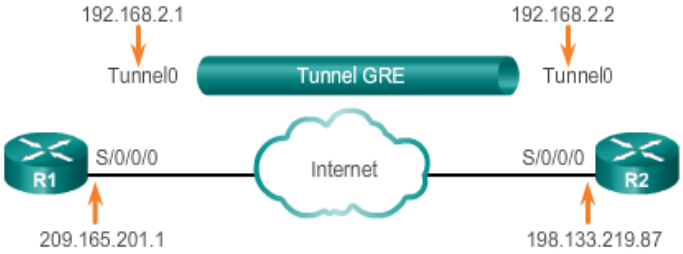
<table>
<tr><td></td><td> 
</td></tr>
<tr><td>VPN d'accès à distance</td><td>- Un VPN d'accès à distance prend en charge les besoins en matière de télétravailleurs, d'utilisateurs mobiles, d'extranet et de trafic entre les consommateurs et les entreprises.
- Les VPN d'accès à distance prennent en charge une architecture client-serveur, dans laquelle le client VPN (hôte distant) obtient un accès sécurisé au réseau de l'entreprise par l'intermédiaire d'un périphérique de serveur VPN à la périphérie du réseau.
- Il se peut qu'un logiciel client VPN doive être installé sur le périphérique final de l'utilisateur mobile (ex. le logiciel Cisco AnyConnect Secure Mobility Client).
 
</td></tr>
</table>

4.4. Tunnels GRE de site à site

- Le protocole **GRE** (Generic Routing Encapsulation) est utilisé pour la création d'un tunnel VPN entre deux sites.
- Pour implémenter un tunnel GRE, on doit tout d'abord apprendre les adresses IP des points d'extrémité.

- Les étapes de configuration de tunnels GRE sont les suivantes :

Etape 1 : Créer une interface de tunnel.	R1(config)# **interface tunnel** *number*
Etape 2 : Spécifier l'adresse IP source du tunnel	R1(config-if)# **tunnel source** *address*
Etape 3 : Spécifier l'adresse IP de destination du tunnel	R1(config-if)# **tunnel destination** *address*
Etape 4 : Configurer l'adresse IP pour l'interface du tunnel	R1(config-if)# **ip address** *address masque*
Etape 5 (facultatif) : Spécifier le mode d'interface de tunnel comme étant GRE (c'est le mode par défaut du Cisco IOS)	R1(config-if)# **tunnel mode gre ip**
Etape 6 : Vérification de tunnel GRE	R1#**show ip interface brief** R1# **show interface tunnel 0**




```
R1(config)# interface Tunnel0
R1(config-if)# tunnel mode gre ip
R1(config-if)# ip address 192.168.2.1 255.255.255.0
R1(config-if)# tunnel source 209.165.201.1
R1(config-if)# tunnel destination 198.133.219.87
R1(config-if)# router ospf 1
R1(config-router)# network 192.168.2.0 0.0.0.255 area 0
```

```
R2(config)# interface Tunnel0
R2(config-if)# tunnel mode gre ip
R2(config-if)# ip address 192.168.2.2 255.255.255.0
R2(config-if)# tunnel source 198.133.219.87
R2(config-if)# tunnel destination 209.165.201.1
R2(config-if)# router ospf 1
R2(config-router)# network 192.168.2.0 0.0.0.255 area 0
```

4.5. Protocole IPsec

Voir la suite