Haute école d'ingénierie et d'architecture Fribourg
Hochschule für Technik und Architektur Freiburg

Réseaux IP

414. NAT & PAT

Hes·so FRIBOURG FREIBURG
Haute Ecole Spécialisée de Suisse occidentale
Fachhochschule Westschweiz
University of Applied Sciences and Arts Western Switzerland

Réseaux IP

414. Network Address Translation (NAT) & Port Address Translation (PAT)

Introduction, Principe, Utilité

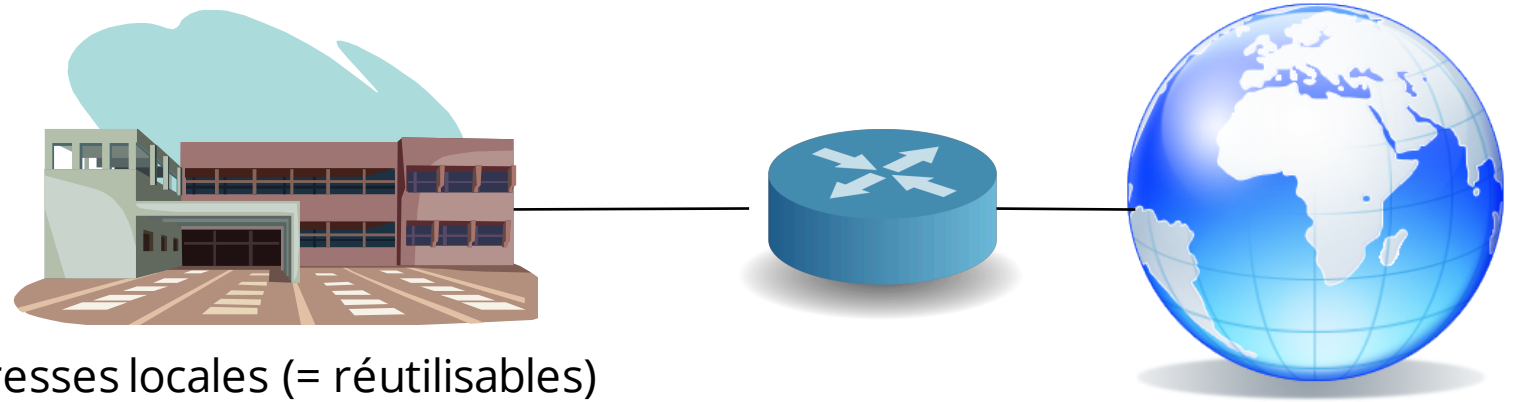
Références:

- **Les Réseaux** (Edition 2005, Pujolle, ISBN 2-212-11437-0).
- **Computer Networks, a system approach** (Edition 4, Larry L. Peterson and Bruce S. Davie, ISBN-13 978-0-12-370548-8)
- **Internetworking with TCP/IP, 4th. Ed**.,(D. Comer, Prentice-Hall).
- **TCP/IP running a successful network**. (K. Washburn and J. Evans, Addison-Wesley, 1996)
- **RFC 3022**

Network Address Translation (NAT)

Translation d'adresses IP entre deux réseaux (définie dans RFC3022). Le NAT (ou aussi appelé **NAT44**) est implémenté dans le routeur qui fait la frontière entre les deux réseaux. Typiquement utilisé pour l'accès à Internet. La translation d'adresses peut être statique (1 à 1) ou dynamique (*All pool*) avec temporisateur (*timeout*).

Inside Network ***Outside Network***



Adresses locales (= réutilisables)

Adresses privées, non-enregistrées, de quelqu'un d'autre, ...

Adresses globales
(= enregistrées)

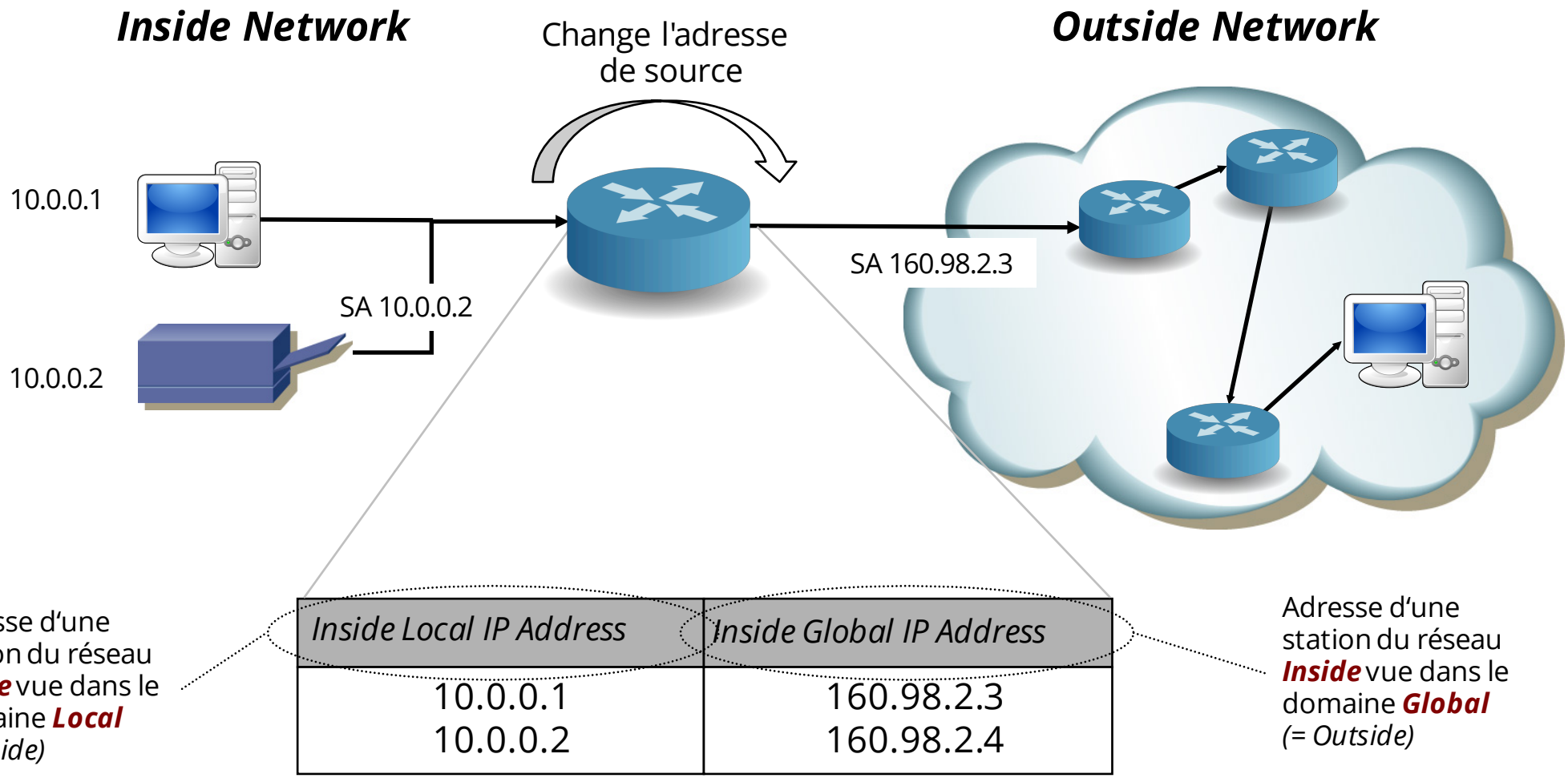
Inside/Outside = « *où est la station* »
Local/Global = « *où sont vues les adresses* »

Motivations du NAT

- Considérations de **sécurité**: cache les adresses "*inside*" au monde extérieur
- **Économise** des adresses IP
- Permet à un réseau d'accéder à Internet sans devoir **enregistrer** toutes les adresses de sous-réseaux auprès de l'autorité d'attribution d'adresses Internet
- Permet de connecter deux réseaux qui ont des **adresses identiques**
- Permet de garder un groupe d'adresse après un changement d'ISP

NAT peut être complété par le NAPT (Network Address and Port Translation)
ou PAT (*Port Address Translation*) qui opère un multiplexage basé sur le "*port number*"

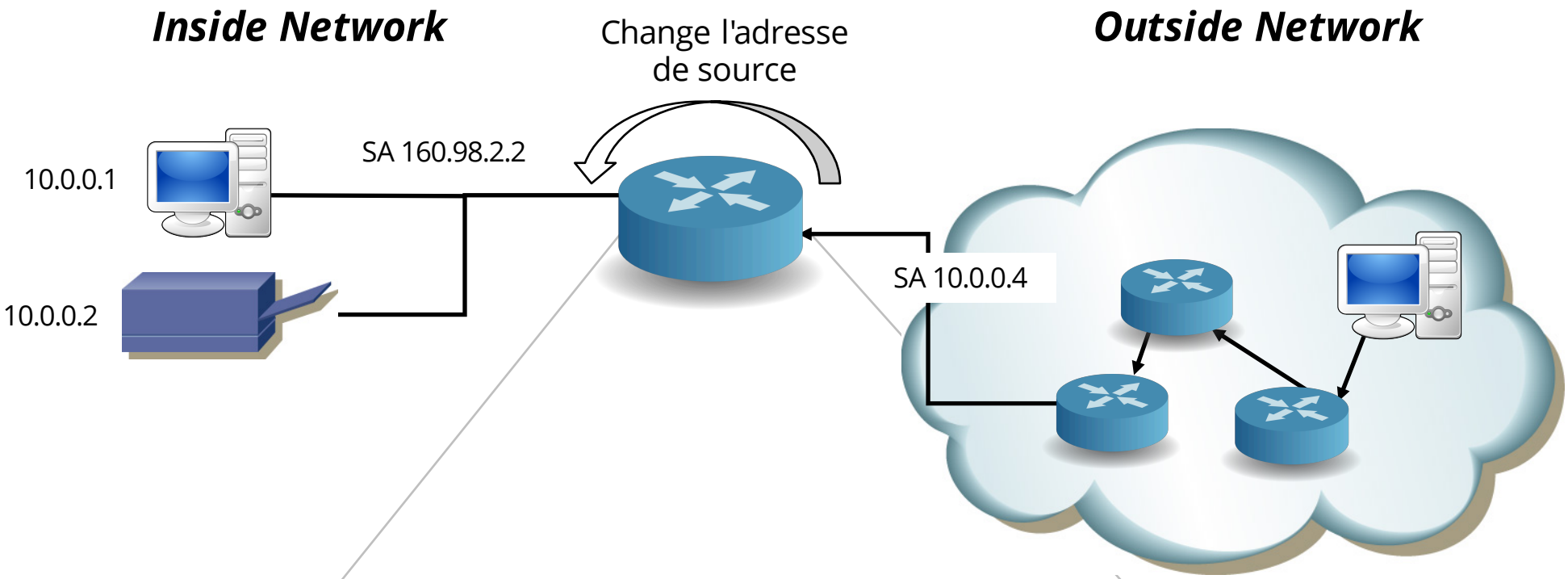
Inside Source Address Translation



Traduction bi-directionnelle: en sens inverse, l'adresse de destination est changée

SA: Source Address

Outside Source Address Translation

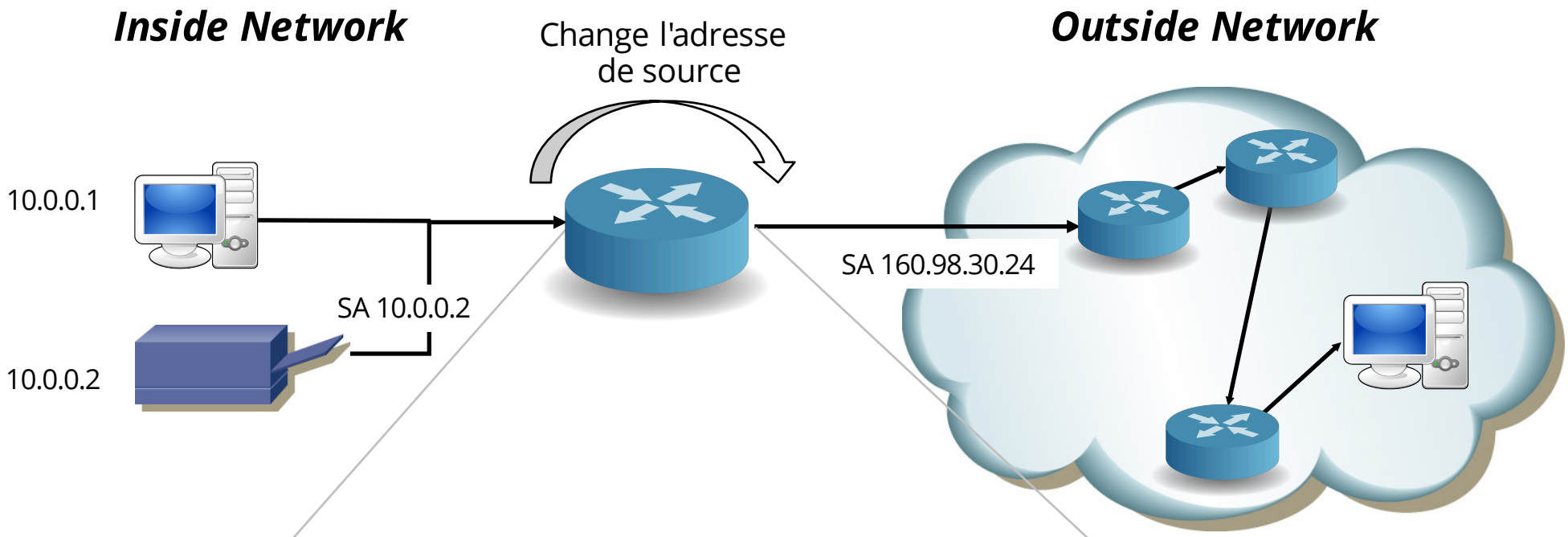


Outside Local IP Address	*Outside Global IP Address*
160.98.2.2	10.0.0.4

Permet d'utiliser des blocs d'adresses identiques

Traduction bi-directionnelle: en sens inverse, l'adresse de destination est changée

Port Address Translation (PAT)



Inside Local IP Address	*Inside Global IP Address*
10.0.0.1:1028	160.98.30.24 : 1028
10.0.0.1:1029	160.98.30.24 : 1029
10.0.0.2:1028	160.98.30.24 : 1024

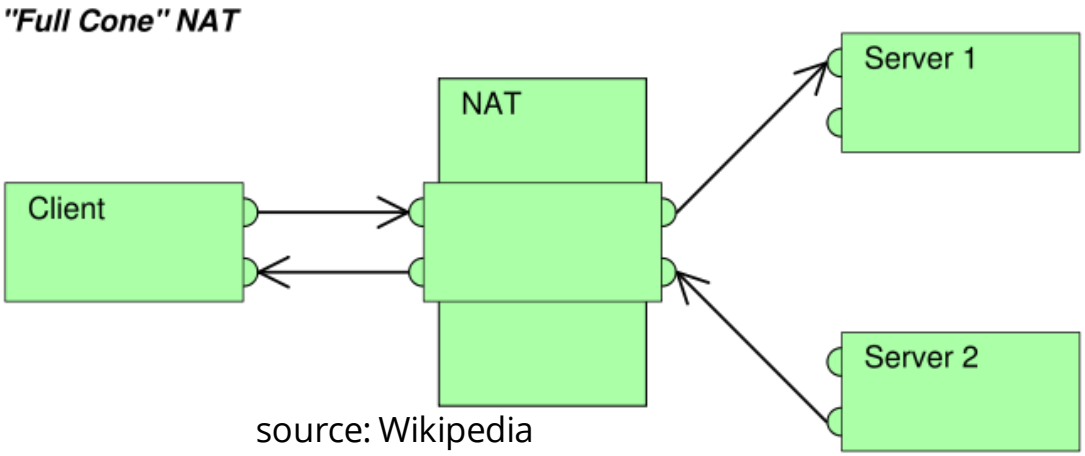
Toutes les stations "internes" utilisent la même adresse IP vu de l'extérieur, multiplexage avec le *Port Number*. PAT utilise en premier le port de source (si pas déjà utilisé pour une autre station source). PAT libère l'entrée dans la table de translation quand le message « FIN » de TCP est observé sur cette connexion.

Variantes du NAT

Bien que le principe du NAT/PAT soit simple, la manière d'assigner une adresse et un port dépend souvent de l'implémentation. Ceci peut avoir des implications importantes lorsque plusieurs flux sont créés par une même machine interne.

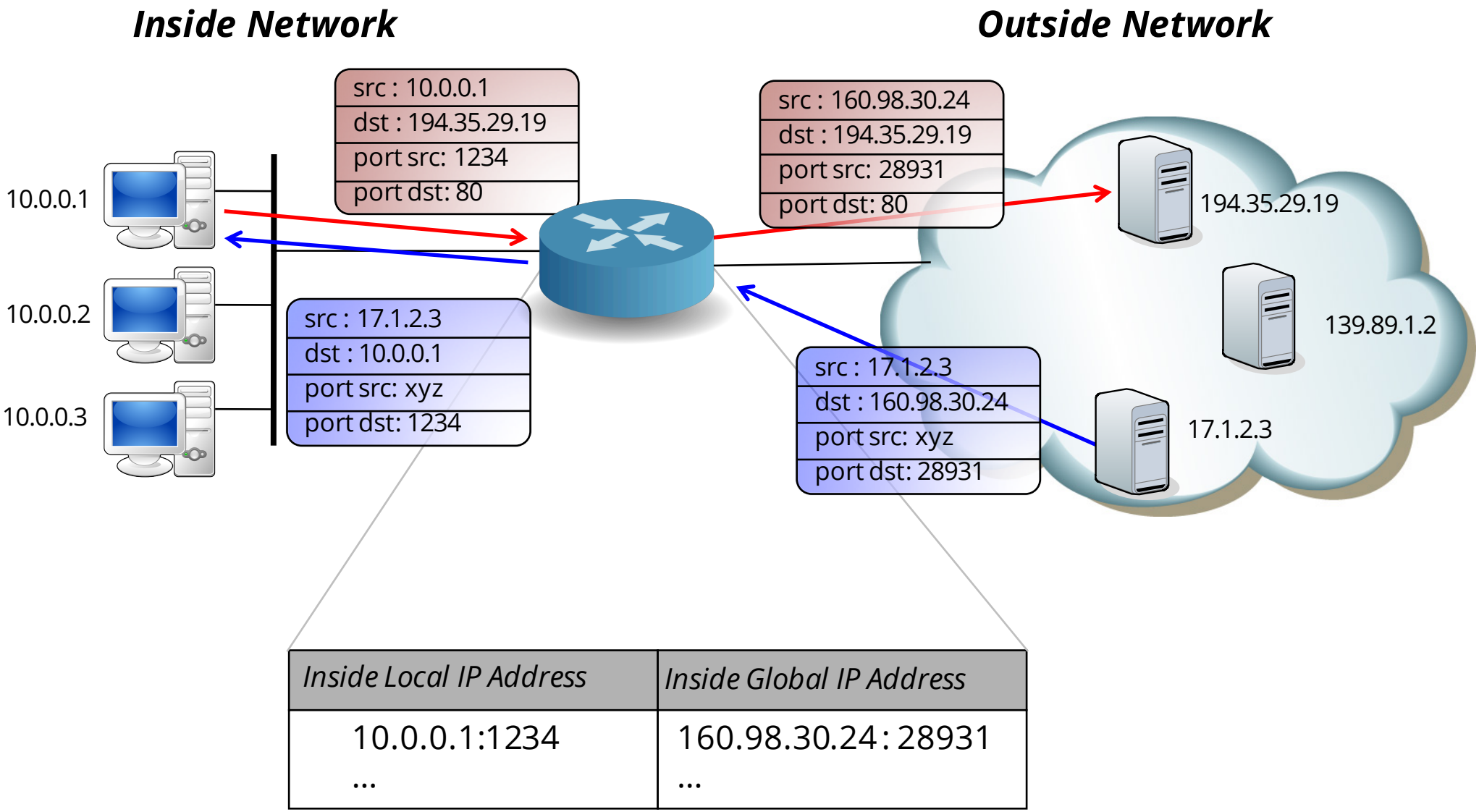
Full cone NAT: Tous les paquets ayant la même paire <adresse source, port source> sont traduits vers la même paire <adresse publique, port source 'public'>, indépendamment du destinataire.

- ➟ N'importe quelle machine externe peut traverser le NAT et atteindre une machine interne en utilisant l'adresse et le port 'public' associés à celle-ci.
- ➟ Méthode simple à implémenter
- ➟ Risque de sécurité élevé !



source: Wikipedia

Full cone NAT



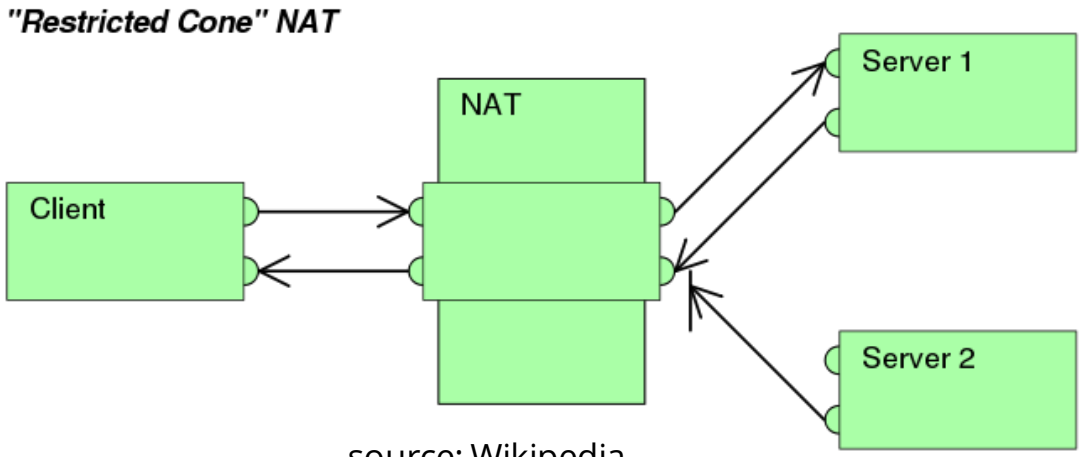
Restricted cone NAT (1)

Restricted cone NAT: Tous les paquets ayant la même paire <adresse source, port source> sont traduits vers la même paire <adresse publique, port source 'public'>, comme dans le cas du Full cone NAT. Les communications « entrantes » sont en plus filtrées.

➡ Seul la machine externe (son adresse IP) pour laquelle le paquet est destiné est autorisée à dialoguer avec le réseau interne.

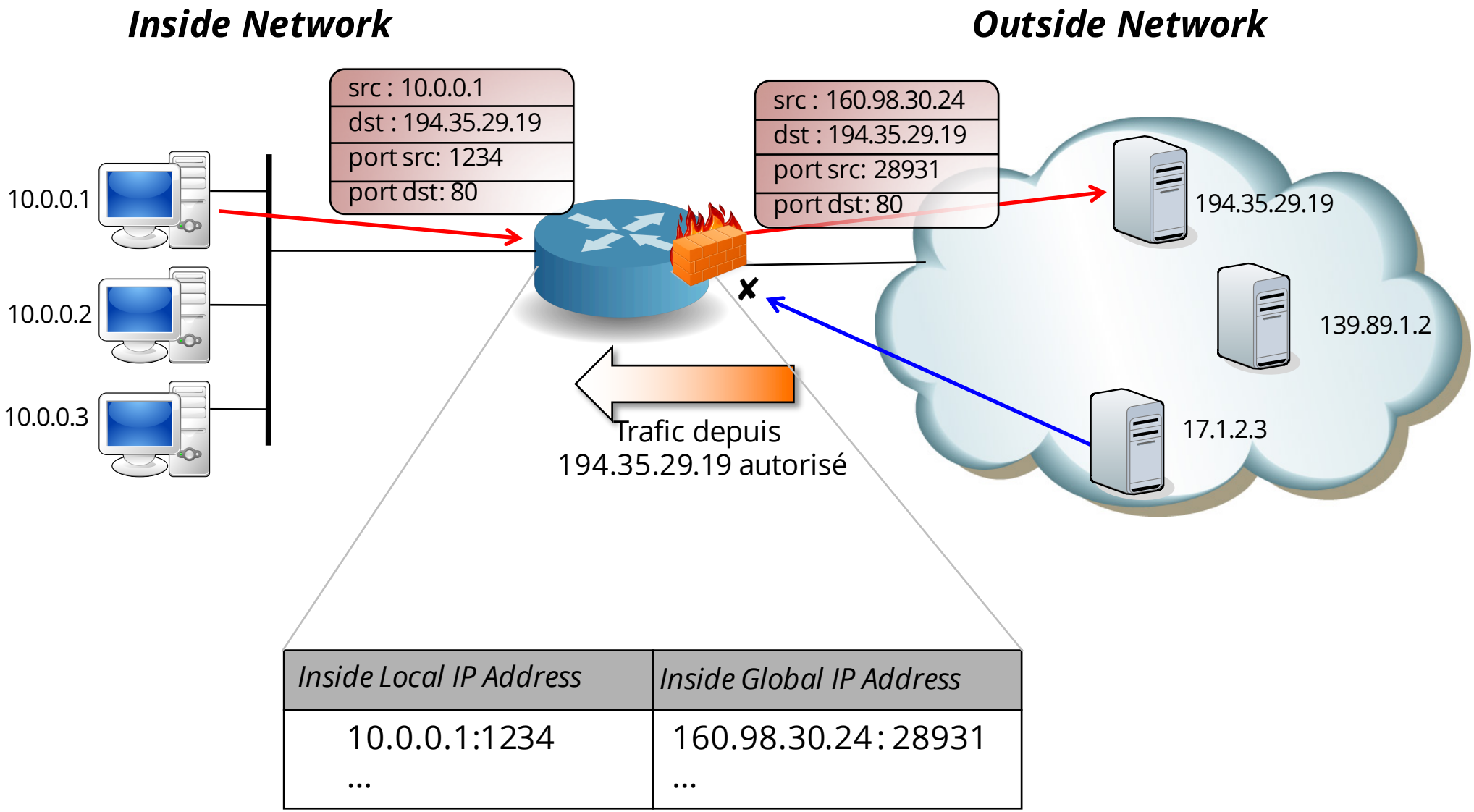
➡ Baisse de performance par rapport au Full cone NAT

➡ Augmentation du niveau de sécurité



source: Wikipedia

Restricted cone NAT (2)



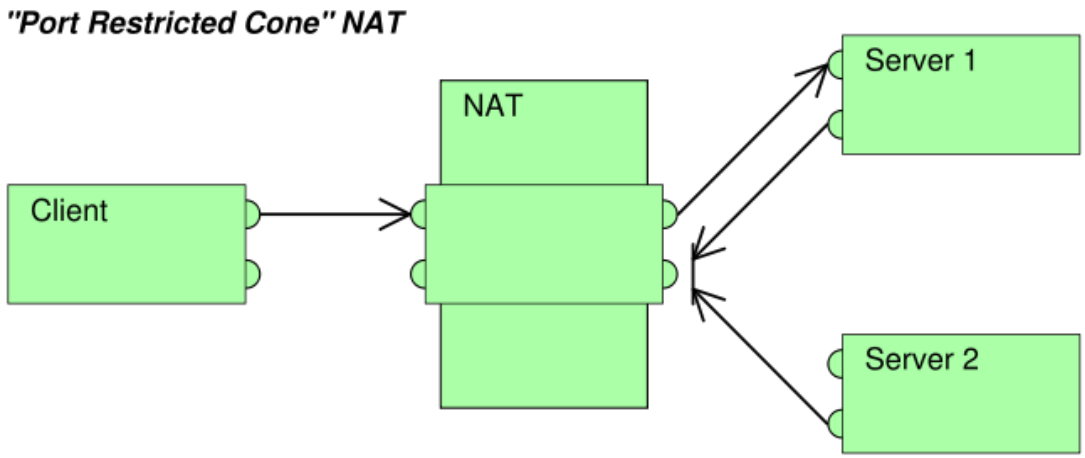
Port restricted cone NAT (1)

Port restricted cone NAT: Similaire au Restricted cone NAT, mais avec une restriction supplémentaire au niveau du port utilisé par la machine externe.

➡ Seul la machine externe (son adresse IP et son port) pour laquelle le paquet est destiné est autorisée à dialoguer avec le réseau interne.

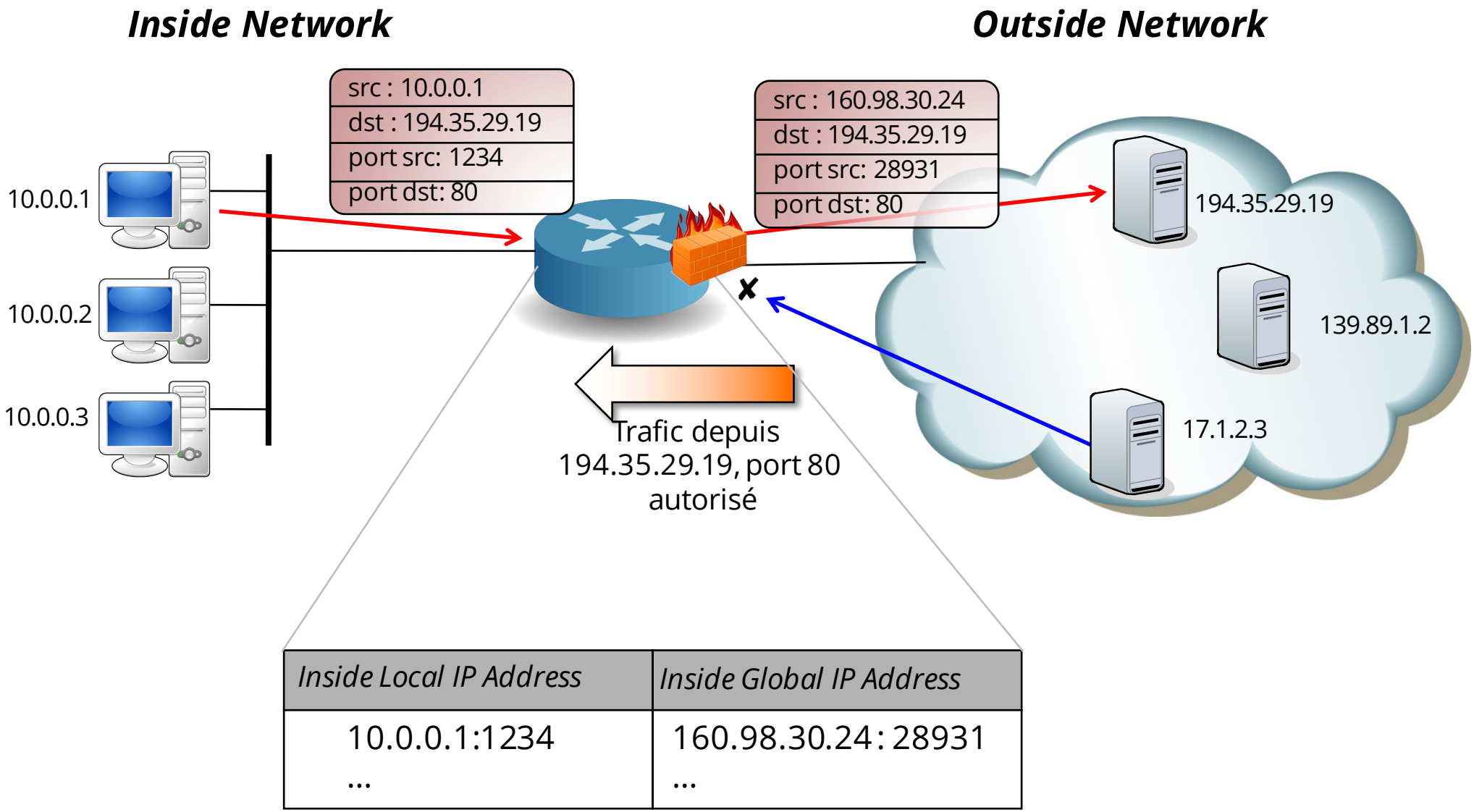
➡ Baisse de performance par rapport au Full cone NAT

➡ Augmentation du niveau de sécurité



source: Wikipedia

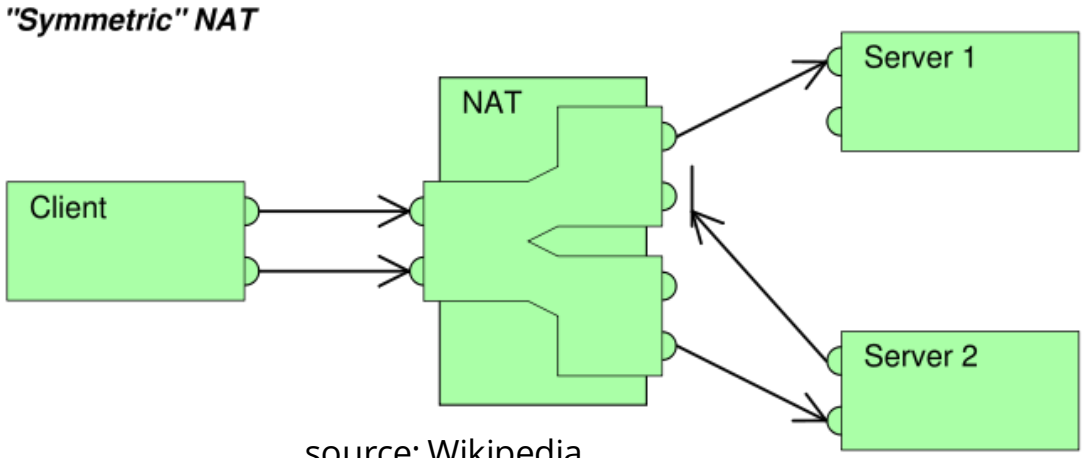
Port restricted cone NAT (2)



NAT symétrique (1)

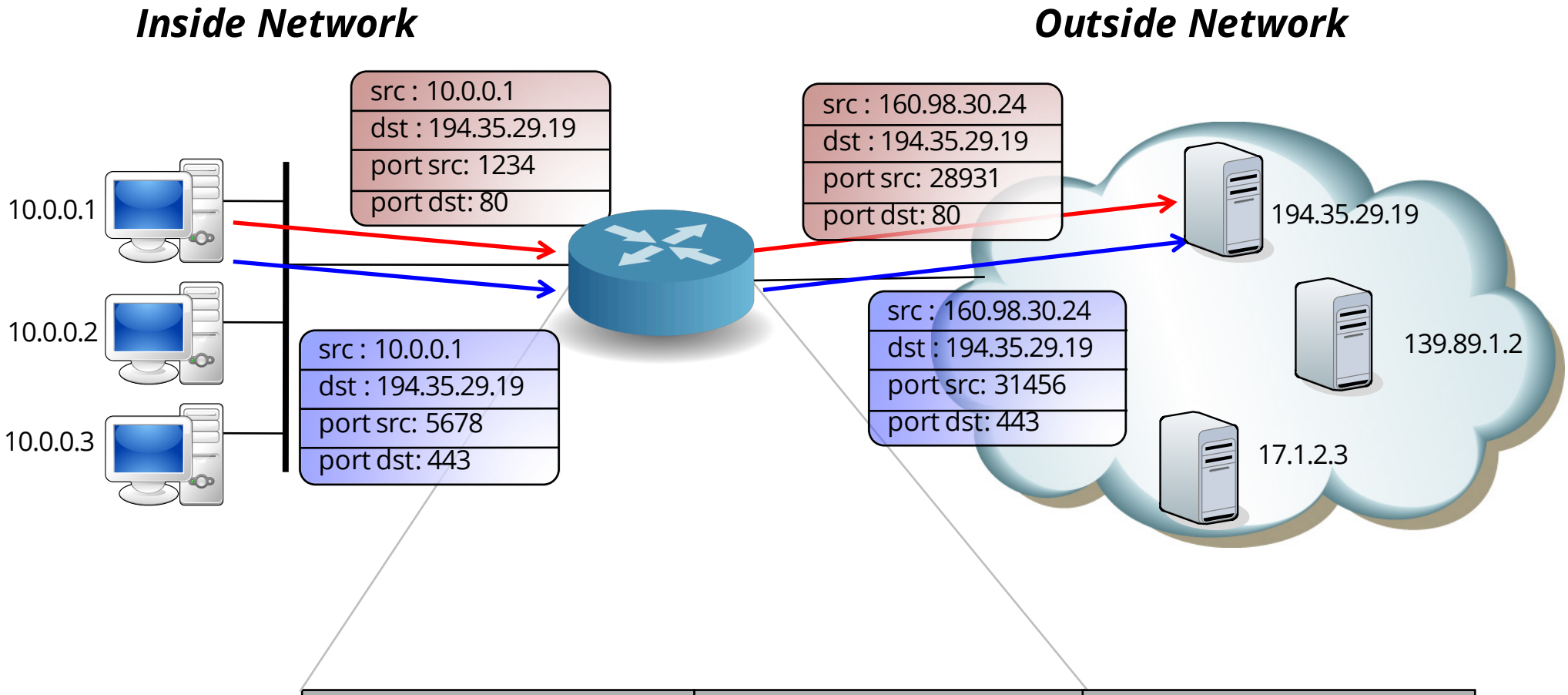
NAT symétrique: Une nouvelle adresse publique ou un nouveau numéro de port source sont utilisés pour chaque destination. La différence avec le Port restricted NAT est qu'une entrée dans la table de translation est créée pour chaque communication.

- ➡ Seul la machine externe (son adresse IP et son port) pour laquelle le paquet est destiné est autorisée à dialoguer avec la machine interne (son adresse IP et son port) qui a initié la connexion .
- ➡ Algorithme complexe à implémenter
- ➡ Augmentation du niveau de sécurité
- ➡ Un numéro de port est « consommé » par flux actif, ce qui limite le nombre de flux simultané à 65535, par adresse IP publique.



source: Wikipedia

NAT symétrique (2)



Inside Local IP Address	*Inside Global IP Address*	*Outside Global IP Address*
10.0.0.1 : 1234 10.0.0.1 : 5678 ...	160.98.30.24 : 28931 160.98.30.24 : 31456 ...	194.35.29.19 : 80 194.35.29.19 : 443 ...

Variantes de NAT: conclusion

Le type de NAT utilisé à un grande influence lors de la réalisation de services avancés comme la téléphonie sur Internet. Le NAT symétrique est souvent utilisé par les entreprises (constructeurs), ce qui pose d'énorme problème lors de l'implémentation de la VoIP.

Une liste indiquant le type de NAT utilisé par les produits les plus populaires est disponible sous:

http://www3.tools.ietf.org/html/draft-jennings-midcom-stun-results-01

Un outil permettant de tester le type de NAT est mis à disposition par les développeurs d'eMule sous:

http://forum.emule-project.net/index.php?showtopic=130035

NAT / PAT : limitations (1)

- **Performance**:
  - Modification des entêtes des paquets
    → **Recalculation du checksum IP & TCP**
  - Modification du numéro de port
    → **Recalculation du checksum TCP**

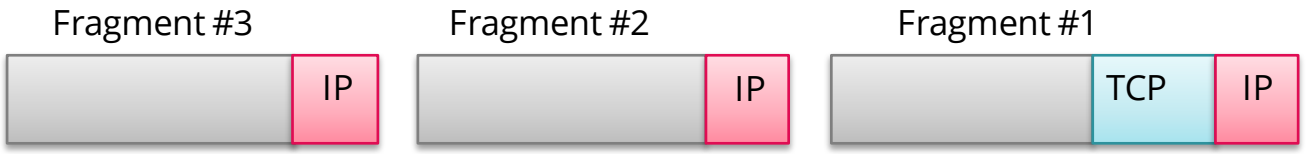
- **Fragmentation**:
  - Tous les fragments devront être translaté vers la même adresse IP

En-tête IP

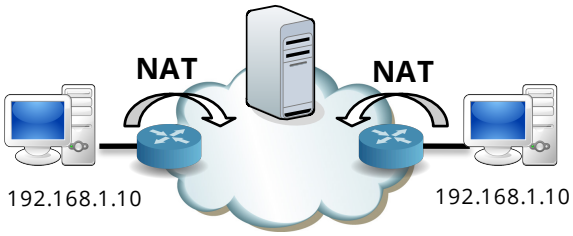
Version	IHL	Type of Service	Total Length
Identification		Flags	Fragment Offset
Time to Live	Protocol	**Header Checksum**	
Source Address			
Destination Address			
Options			Padding

En-tête TCP

Source Port		Destination Port
Sequence number		
Acknowledgement number		
Header length	Flags	Window Size
Checksum		Urgent Pointer
Options (if any)		



NAT / PAT : limitations (2)



- **Connectivité**
  - Accessibilité de bout-en-bout
  - *Comment faire lorsque deux stations voulant communiquer ont des adresses privées ?*

- **Adresse(s) IP dans les "données"**:
  - Transport des adresses IP dans les données en plus de l'entête (par ex. SIP ou IPSec)

- **Implémentations**
  - Diverses méthodes, niveaux de sécurité différents (full cone NAT, Restricted Cone NAT, Port Restricted Cone Nat ou NAT Symétrique)

NAT/PAT exemple

```
thorgal# iptables -t nat --append POSTROUTING -o eth0 -j MASQUERADE
```

```
thorgal# netstat-nat -Nn
Proto NATed Address          NAT-host Address          Destination Address      State
tcp   192.168.166.132:59310  160.98.101.225:59310      173.194.35.24:80         TIME_WAIT
tcp   192.168.166.132:59309  160.98.101.225:59309      173.194.35.24:80         TIME_WAIT
tcp   192.168.166.132:59312  160.98.101.225:59312      173.194.35.24:80         ESTABLISHED
tcp   192.168.166.132:59311  160.98.101.225:59311      173.194.35.24:80         TIME_WAIT
```