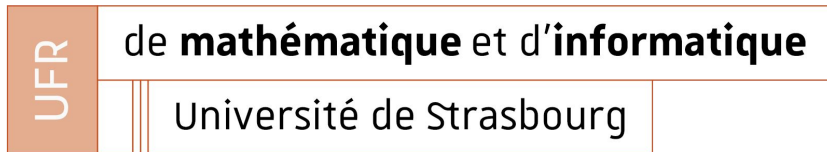


Les NAT sont-ils infranchissables ?

L2S4 PRDS



Par Carine WAKIM & Maxime ZINGRAFF, 23.05.2024
Sujet suivi par M. MONTAVONT

Introduction :

L'essor d'Internet et l'épuisement des adresses IPv4

- Pour **communiquer** sur Internet → **Adresse IP**
(*Internet Protocol*)
- **Protocole IPv4** → **4,3 milliards** d'adresses IP
- Expansion fulgurante d'Internet
 - **Problème** : Pénurie des adresses IPv4
 - **Solution à long terme**: nouveau protocole IP
 - **+ Solutions à court terme** ...

Network Address Translators :

Des solutions provisoires

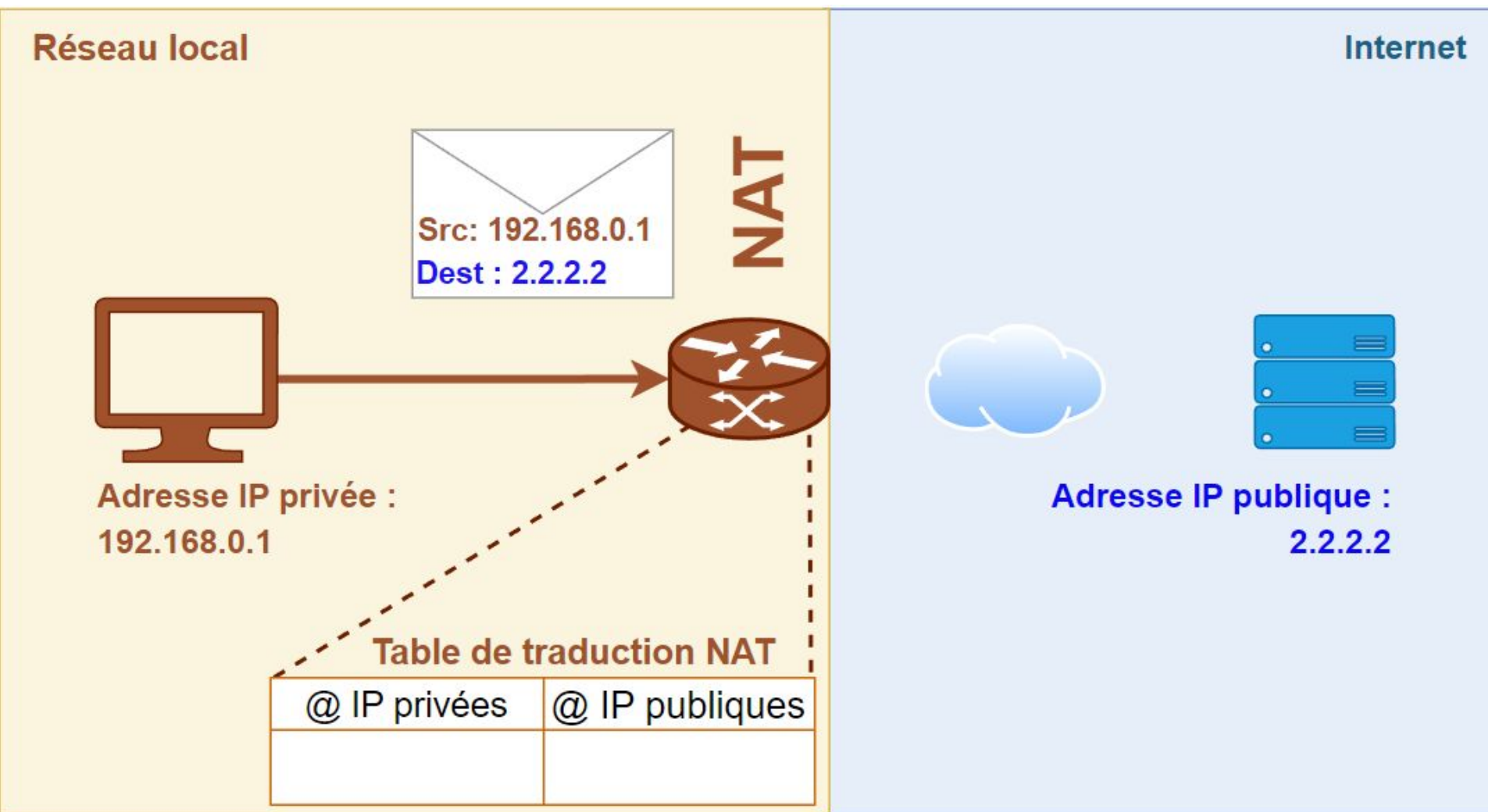
- Les **NAT - *Network Address Translators* (1994)** :
Traduisent les adresses IP privées (non routables) en adresses IP publiques (routables et mondialement uniques)

RFC 1631 “The IP Network Address Translator (NAT)”

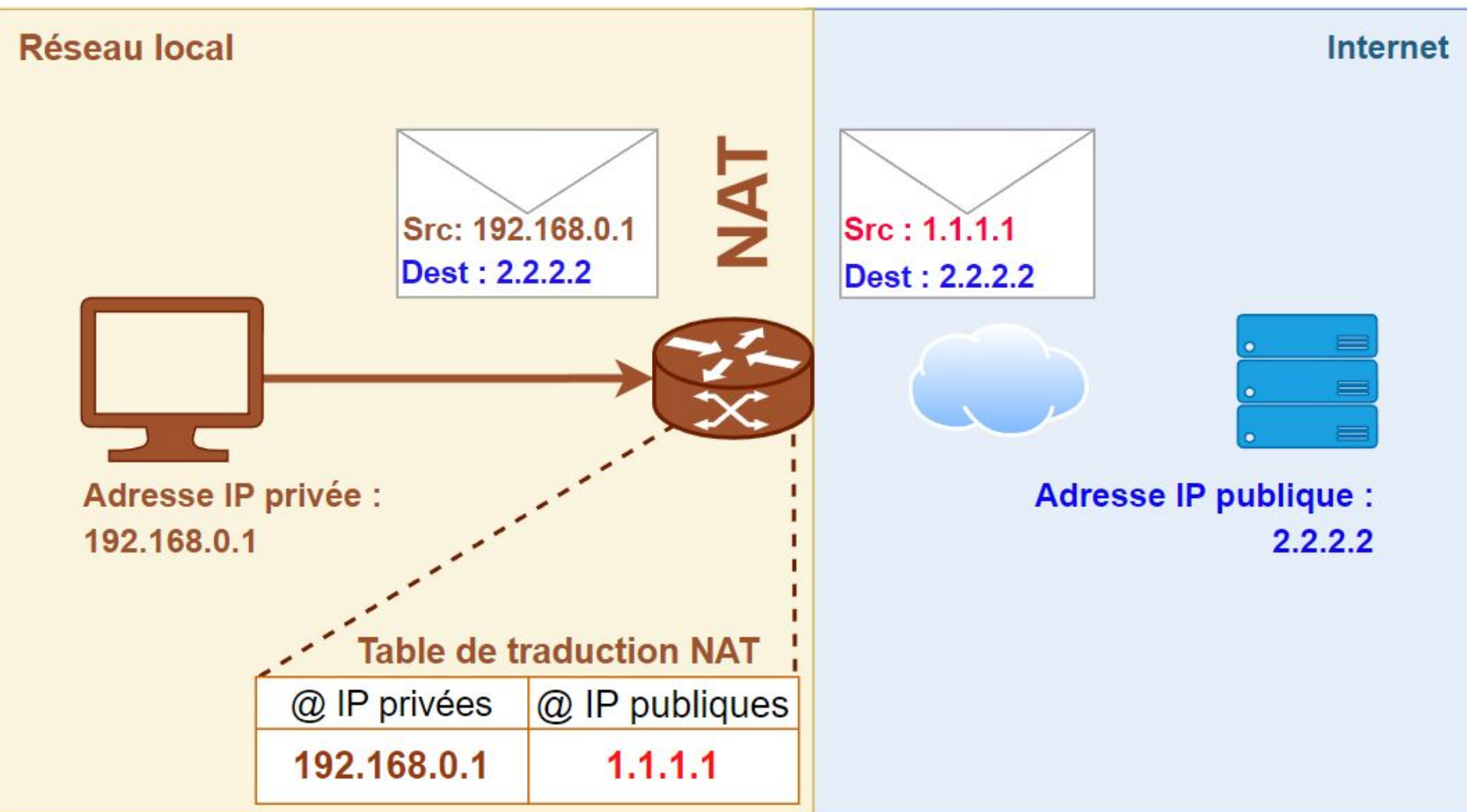
Comment les NAT pallient-ils le manque d'adresses IP ?

- En absence de NAT :
 - 1 appareil = 1 adresse IP publique
 - Gaspillage d'adresses IP
- En présence de NAT :
 - 1 appareil **qui veut communiquer sur Internet** = 1 adresse IP publique
 - Pas de gaspillage d'adresses IP

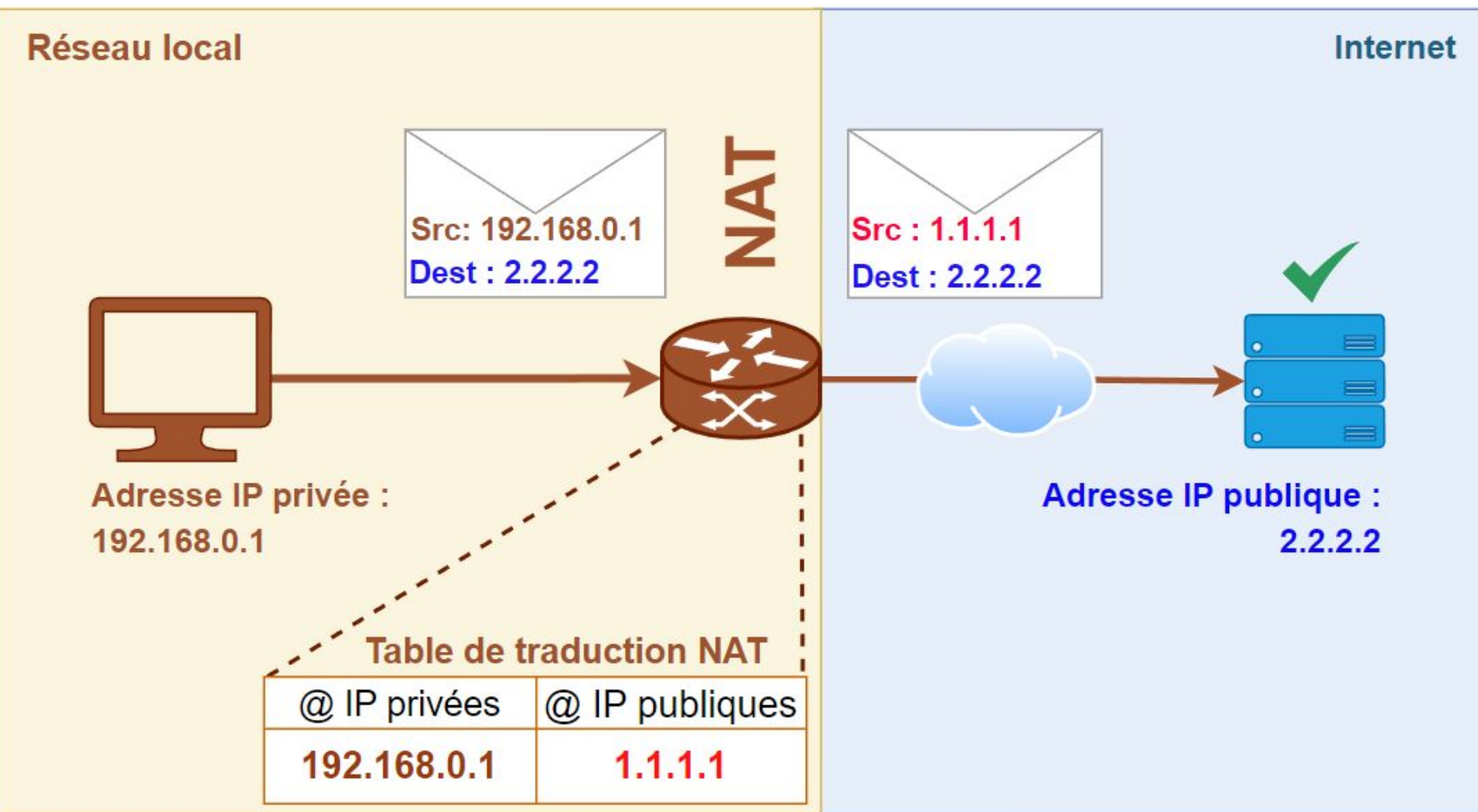
Le fonctionnement effectif des NAT



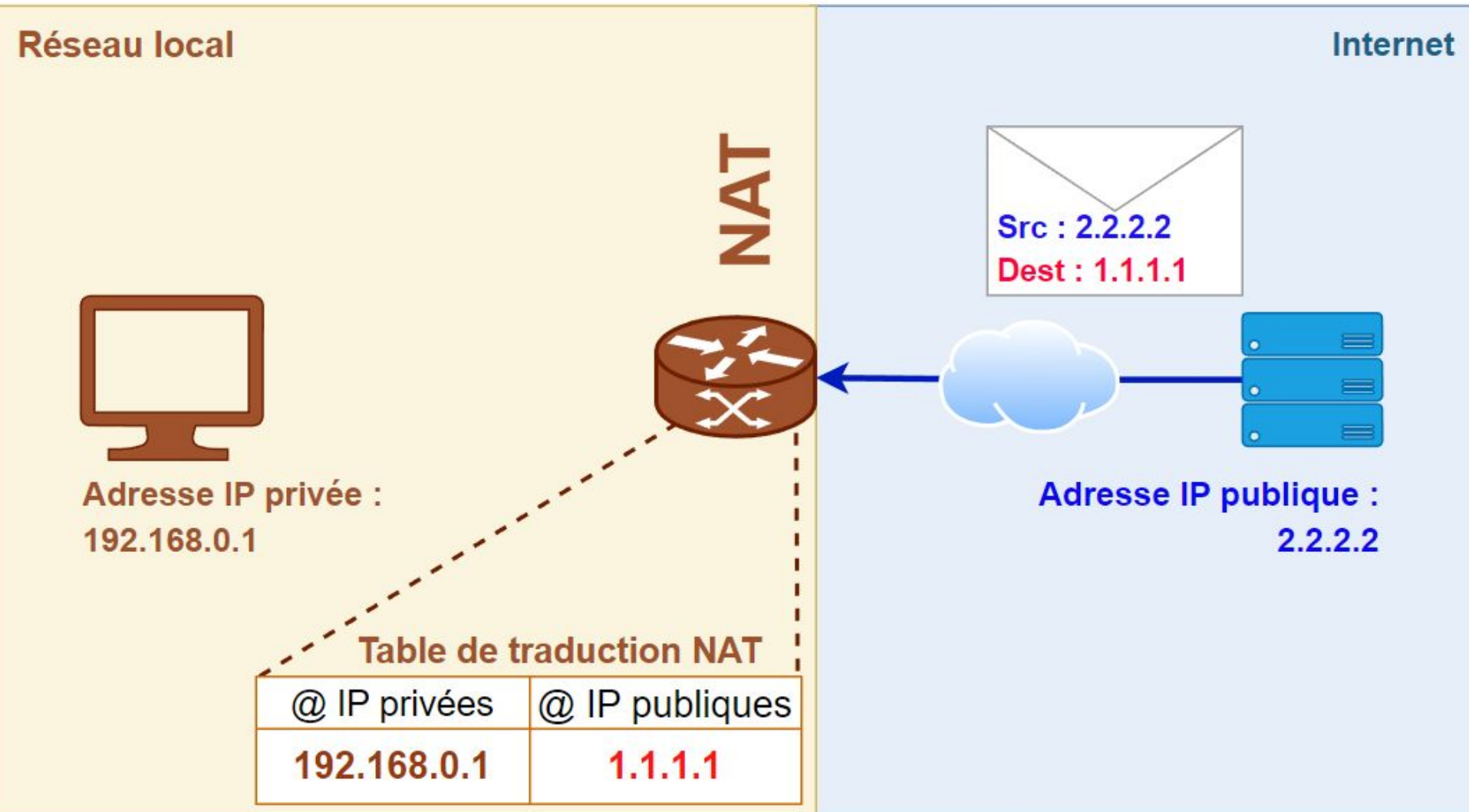
Le fonctionnement effectif des NAT



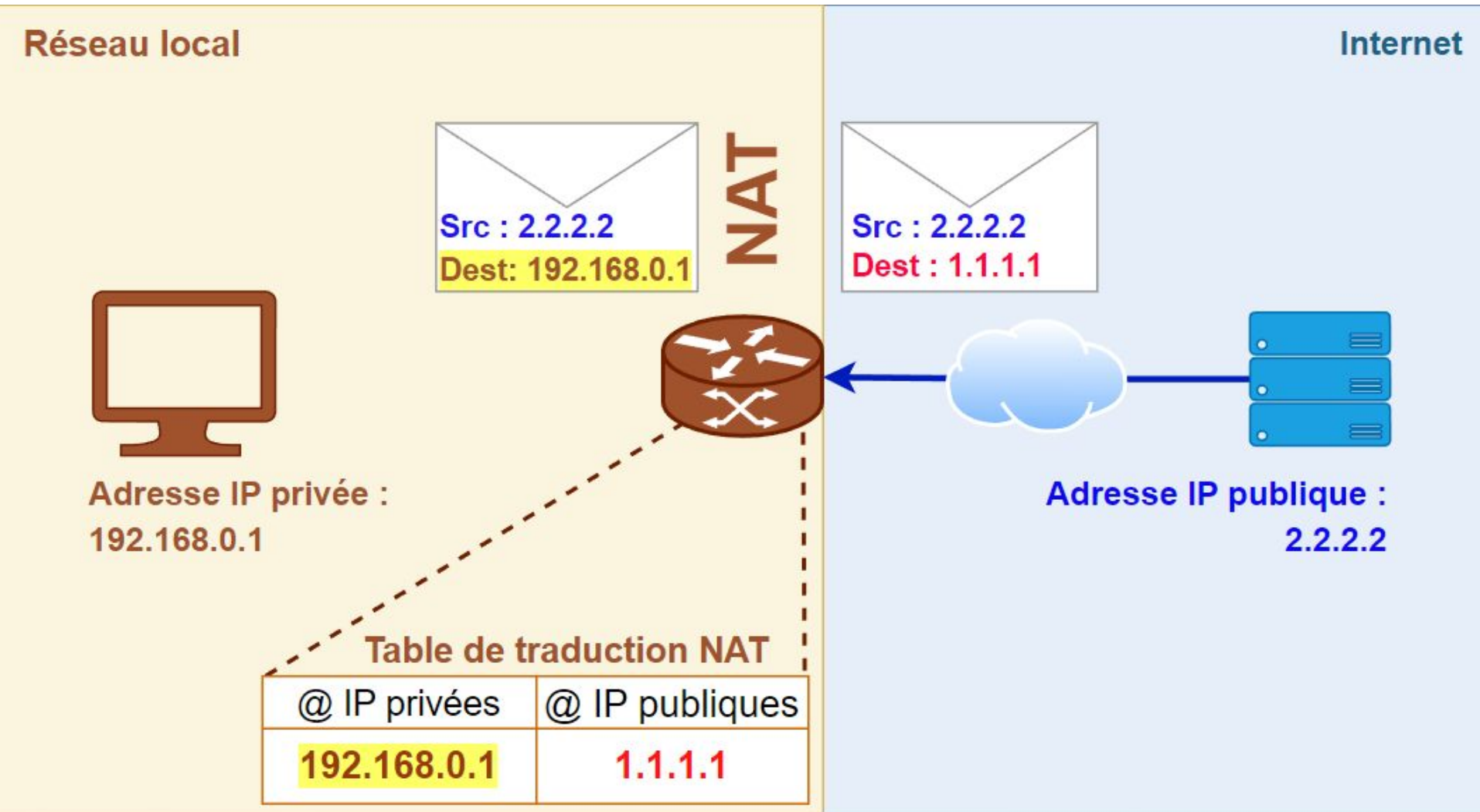
Le fonctionnement effectif des NAT



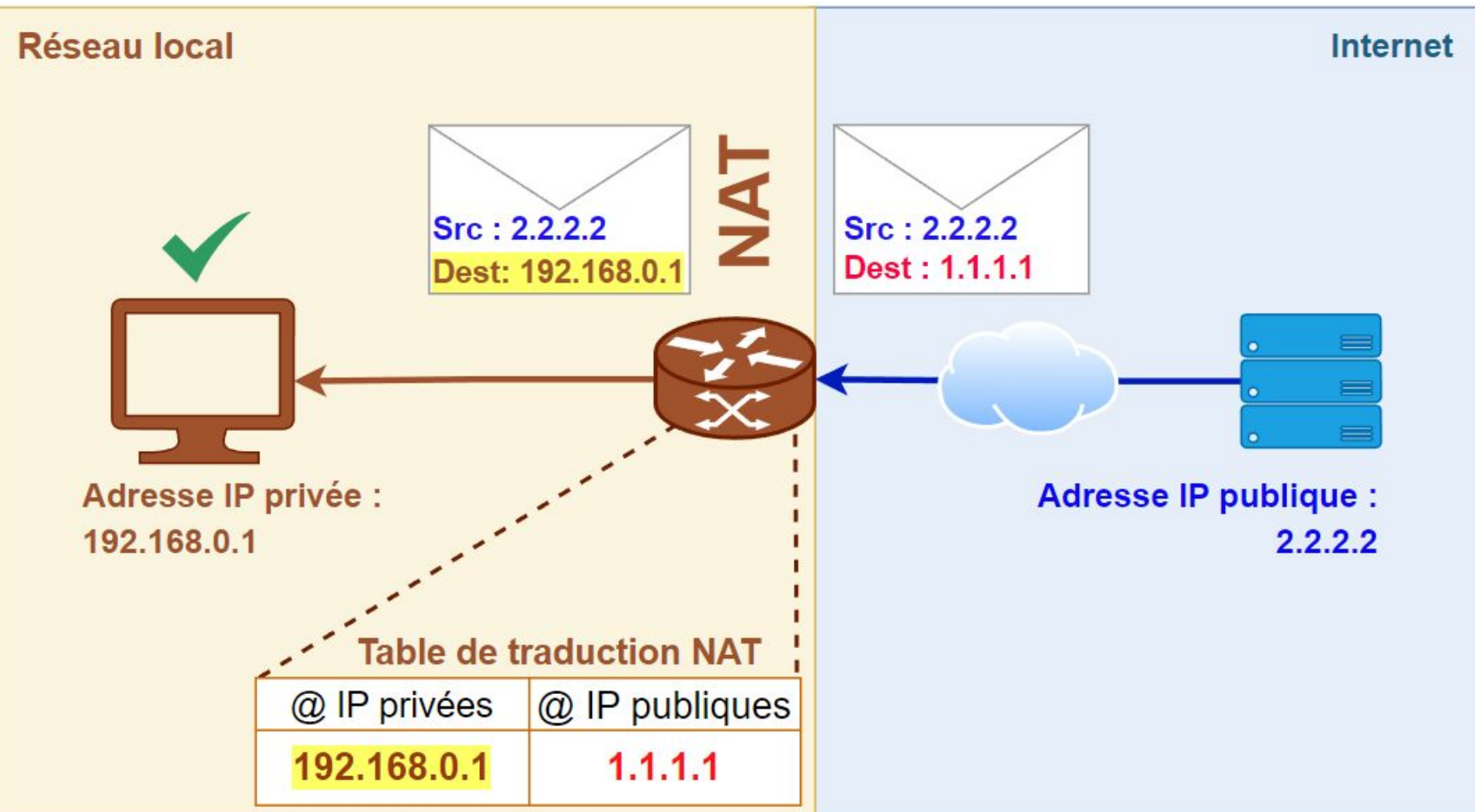
Le fonctionnement effectif des NAT



Le fonctionnement effectif des NAT



Le fonctionnement effectif des NAT



Les NAT, des barrières ?

- Les NAT ont des **effets secondaires** →
Barrières protectrices mais aussi **entravantes**
 - Pourquoi les NAT sont-ils des barrières ?
 - Ces barrières sont-elles infranchissables ?

Différentes nomenclatures informelles

- Pendant longtemps, pas de nomenclature standardisée
- Une classification connue

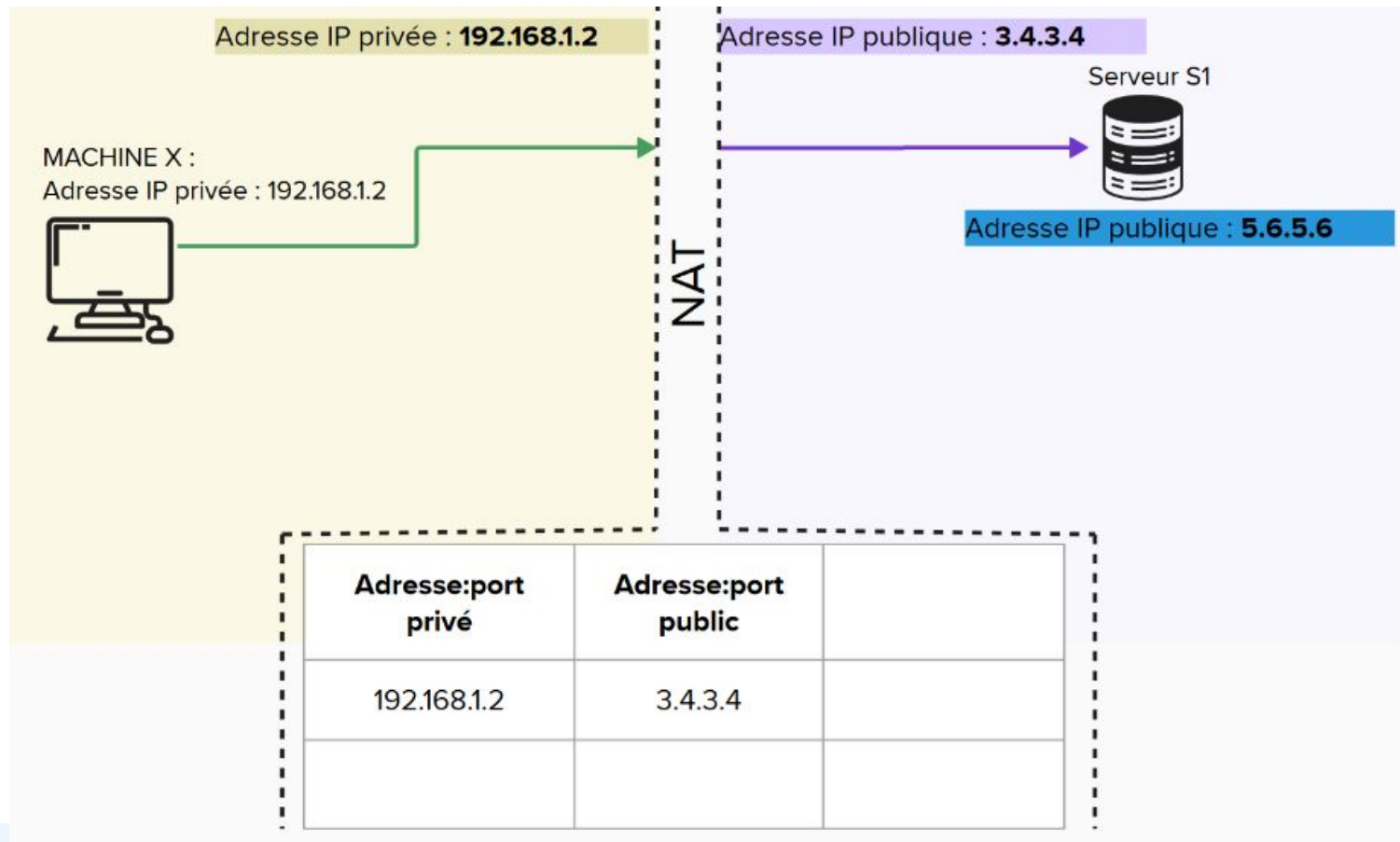
Différentes nomenclatures informelles

- Pendant longtemps, pas de nomenclature standardisée
- Une classification connue
⇒ mais trop technique

Les différents types de NAT

RFC 4787 : Endpoint-Independent Mapping

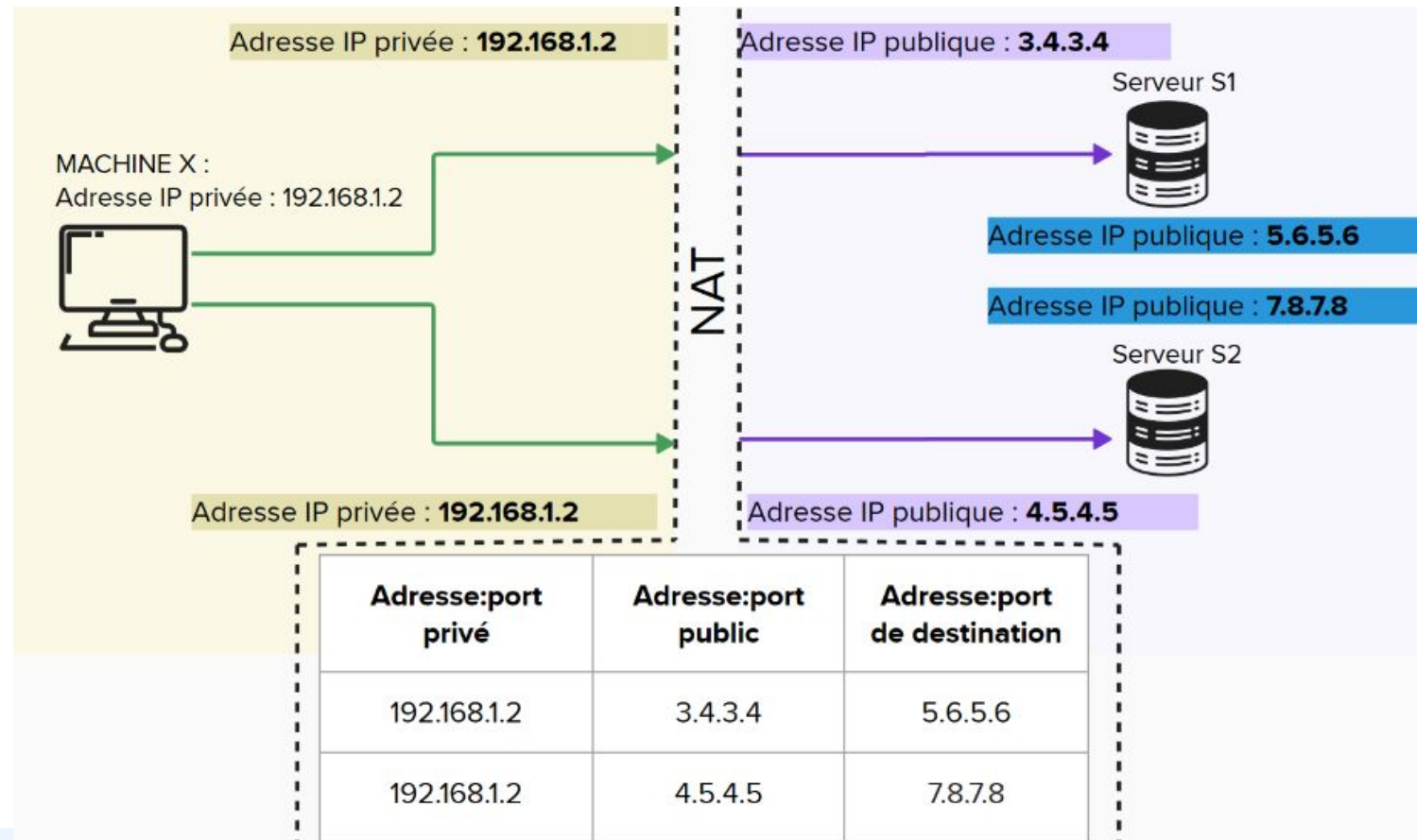
- Simplement, une adresse privée = une adresse publique



Les différents types de NAT

RFC 4787 : Address-Dependent Mapping

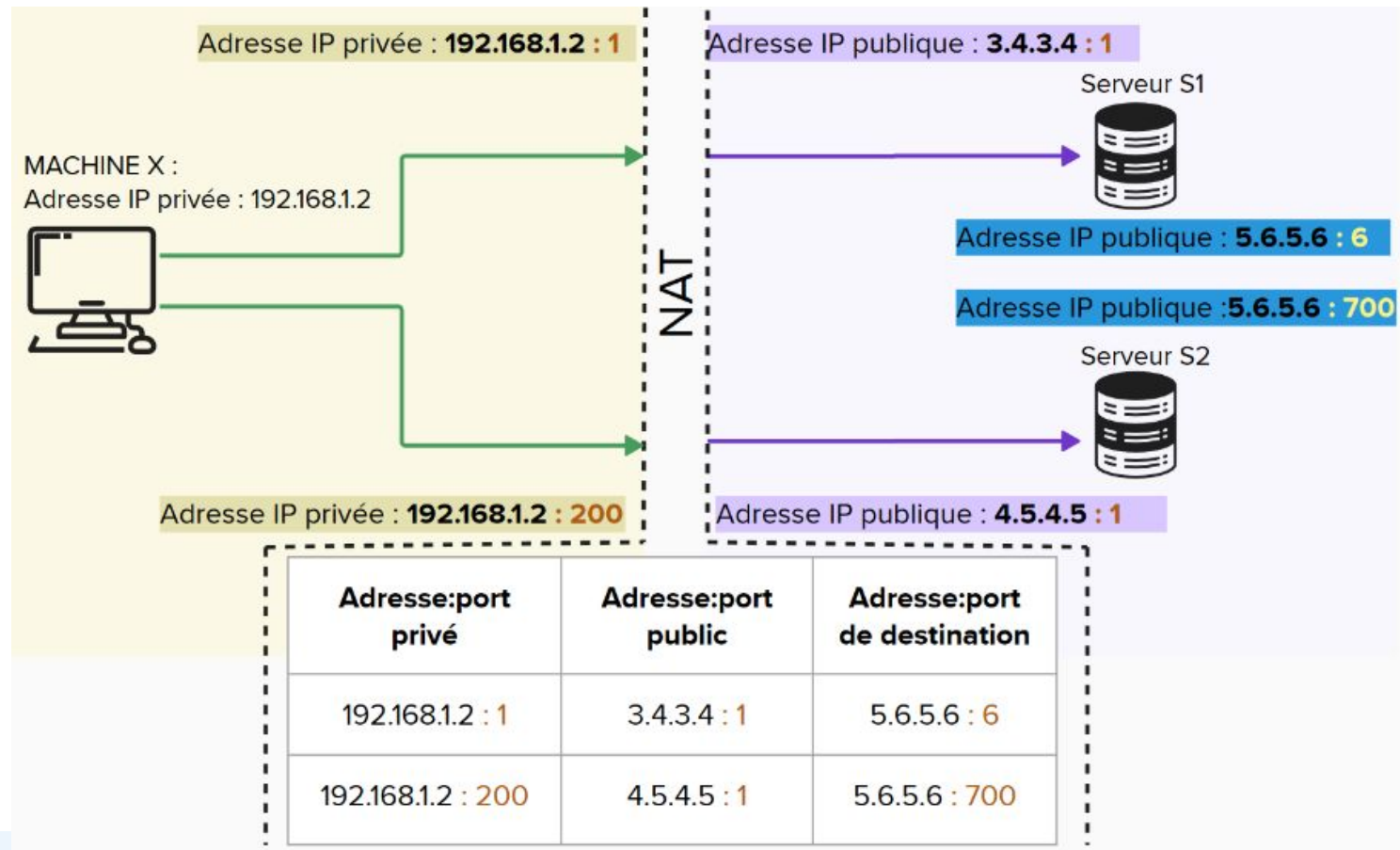
- Une adresse de destination = une adresse publique



Les différents types de NAT

RFC 4787 : Address and Port-Dependent Mapping

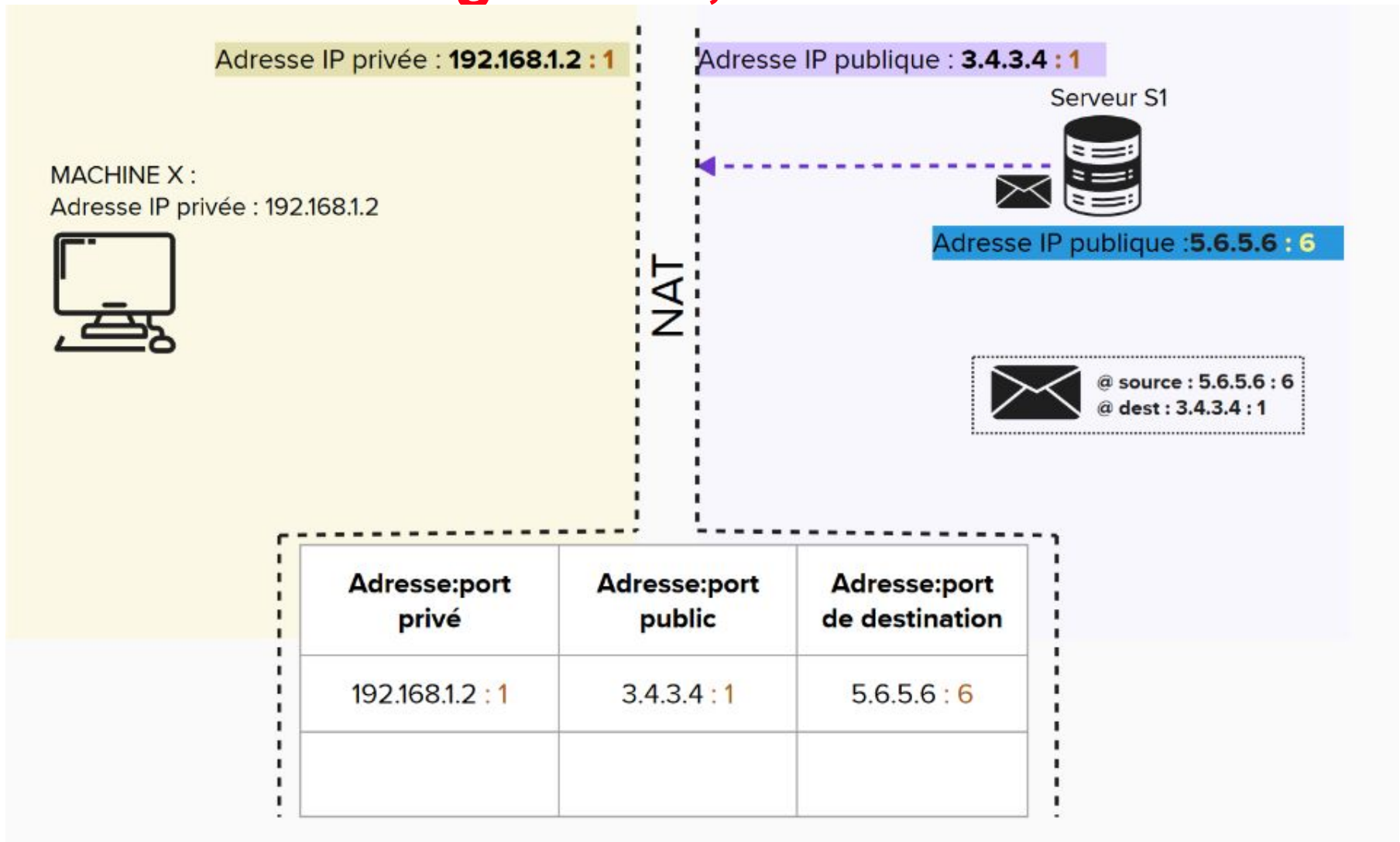
- <adresse:port> de destination = <adresse:port> public



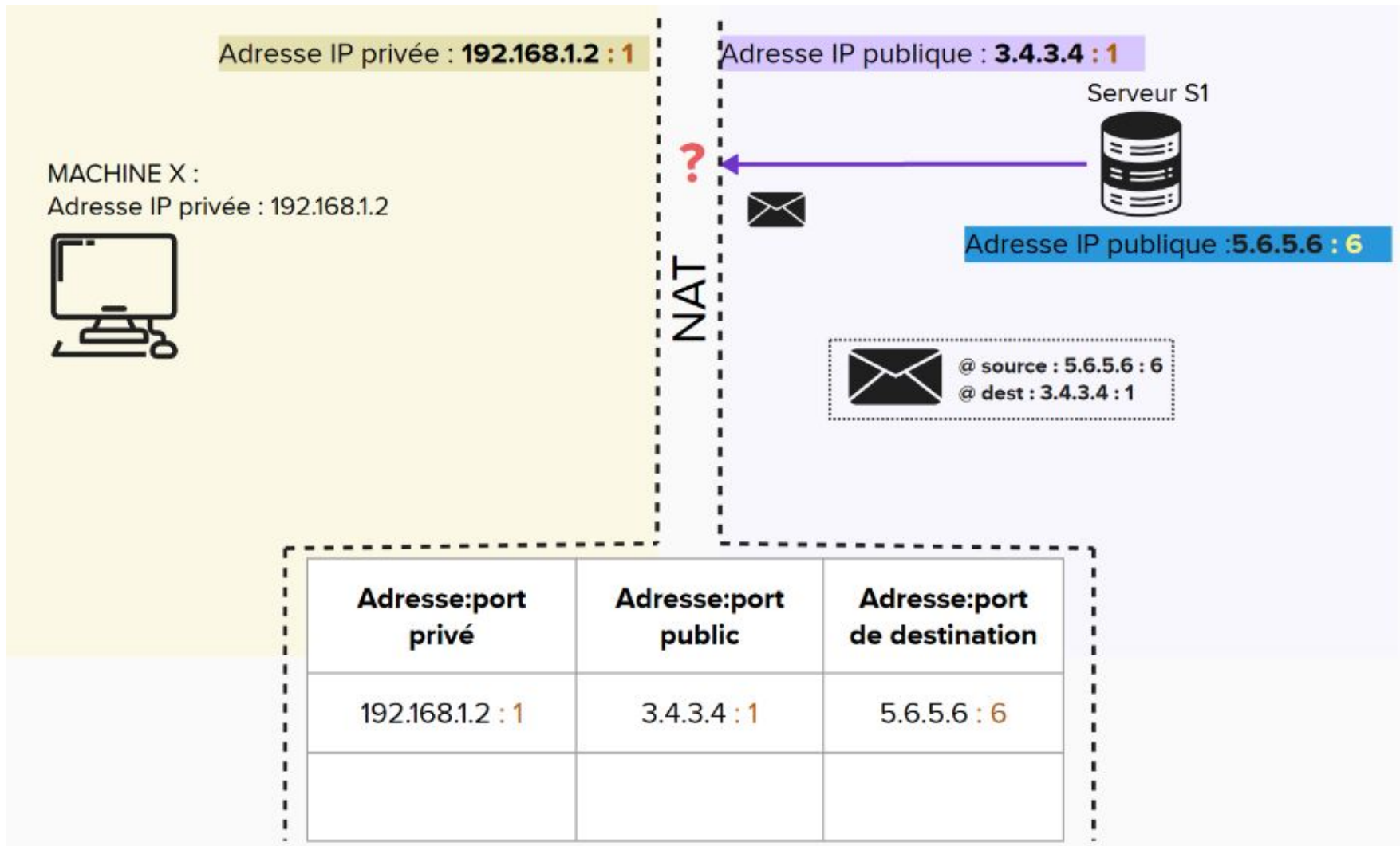
Problèmes engendrés, ou sécurité ?

1. Les NAT brisent le modèle bout en bout
2. Deux types ont des effets secondaires :
 - Address-Dependent Mapping
 - Address and Port-Dependent Mapping

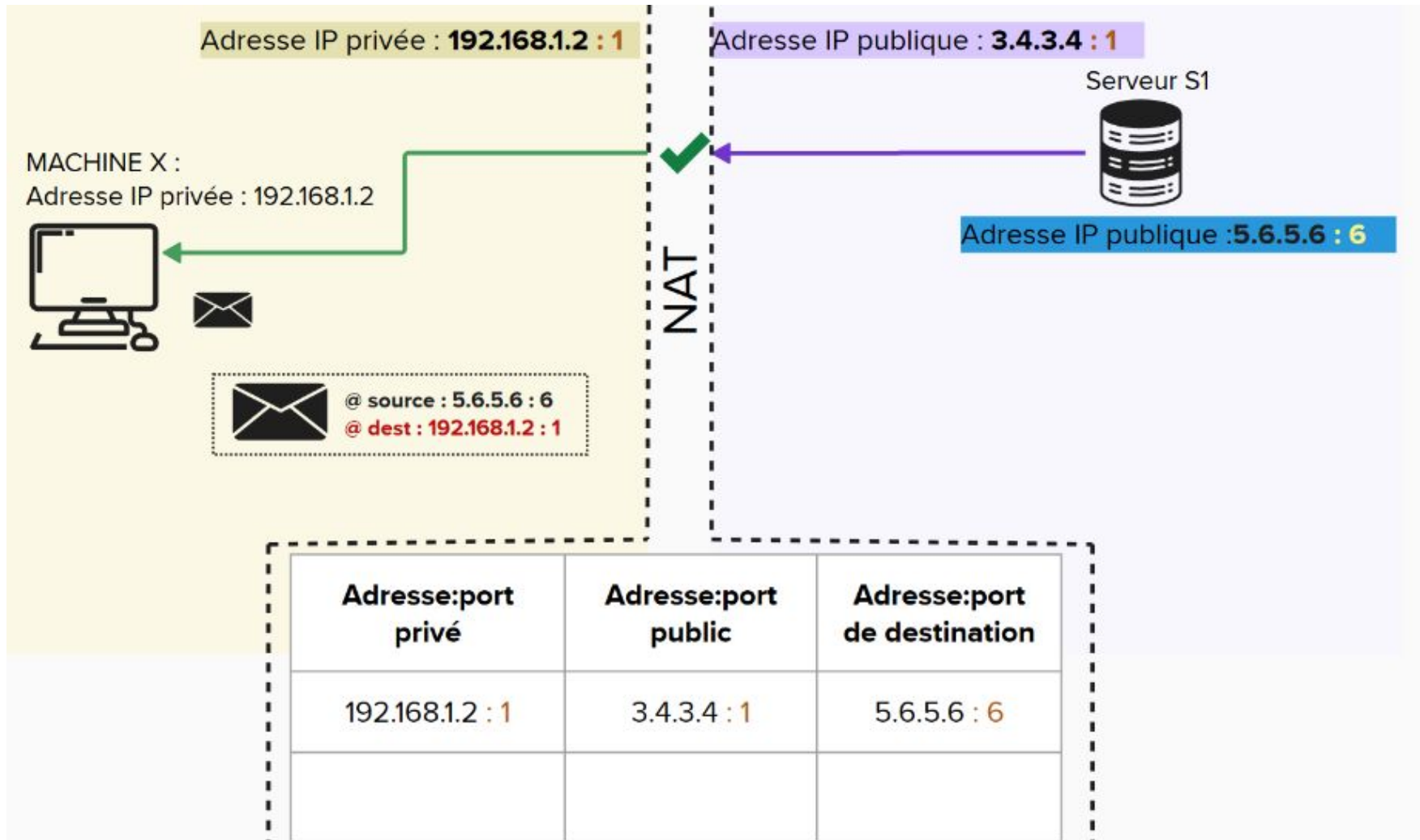
Problèmes engendrés, ou sécurité ?



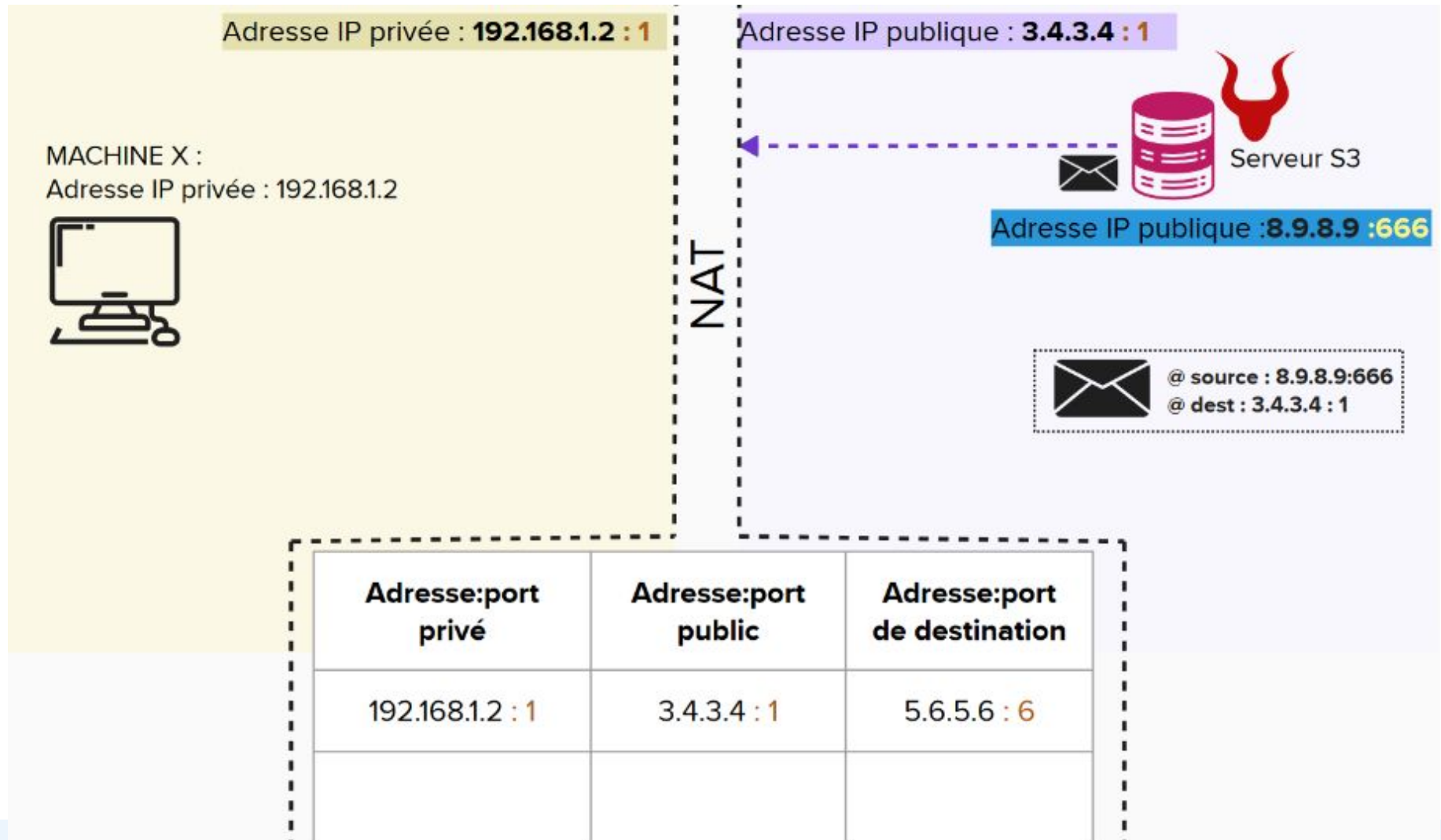
Problèmes engendrés, ou sécurité ?



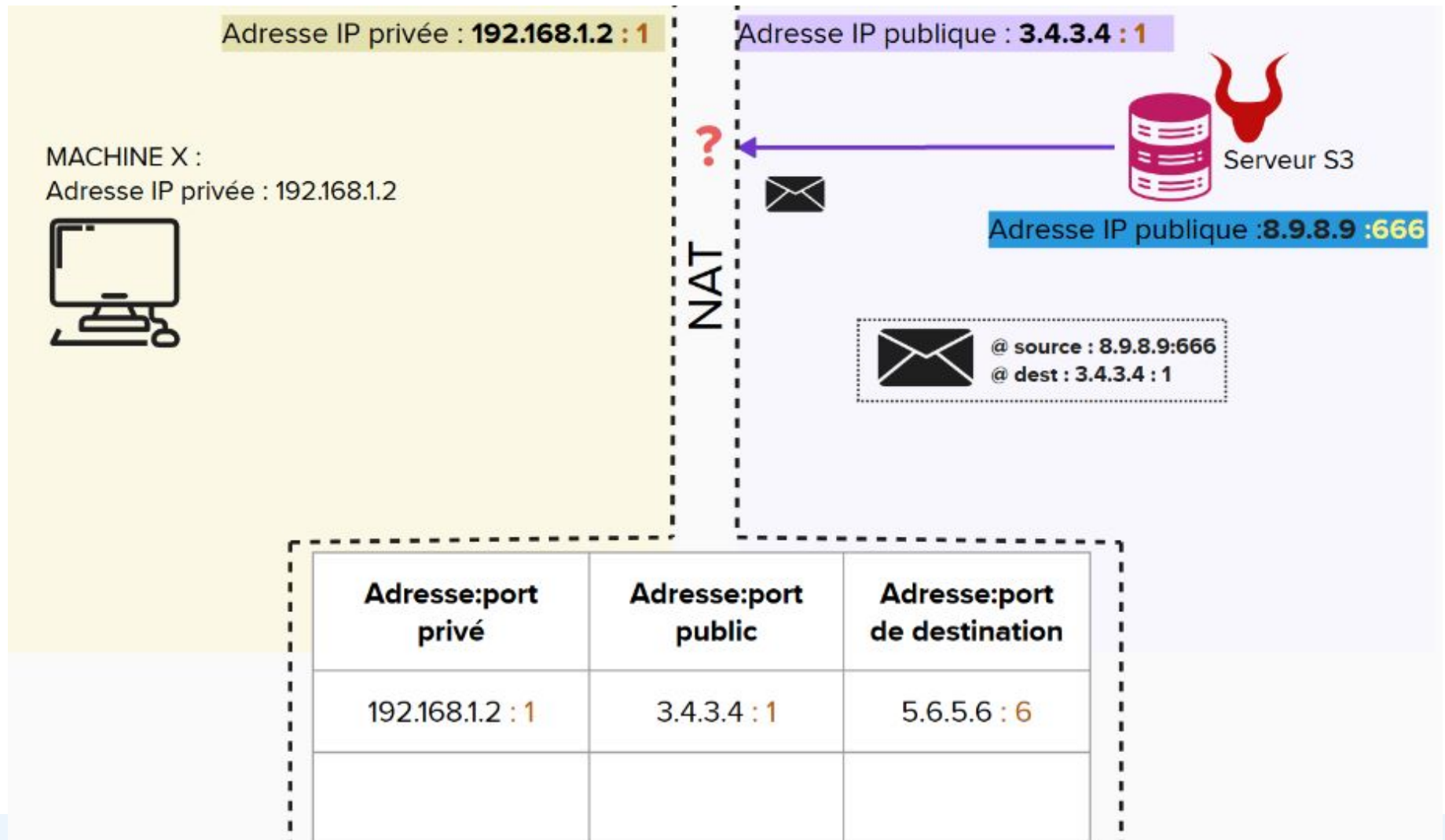
Problèmes engendrés, ou sécurité ?



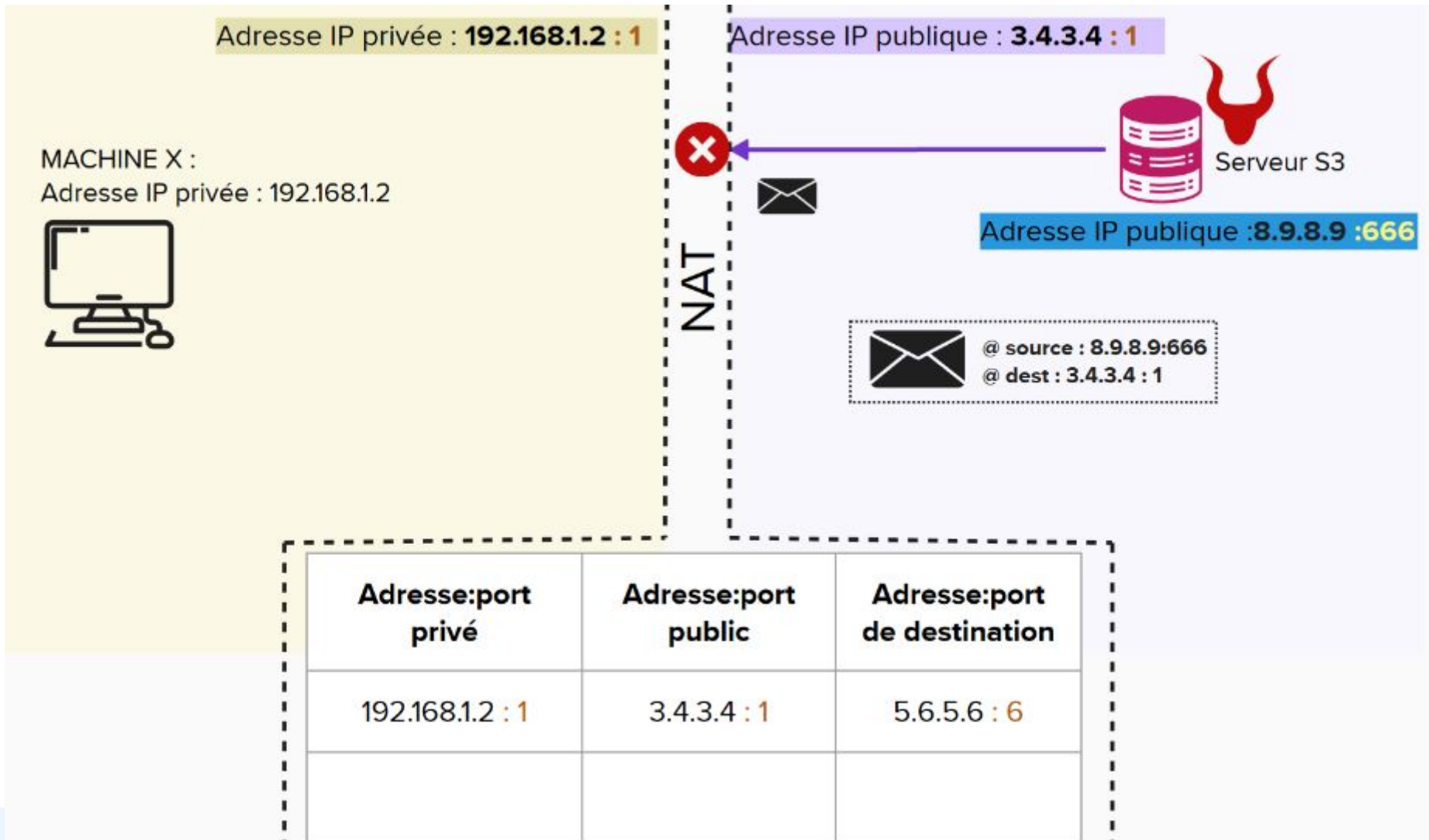
Problèmes engendrés, ou sécurité ?



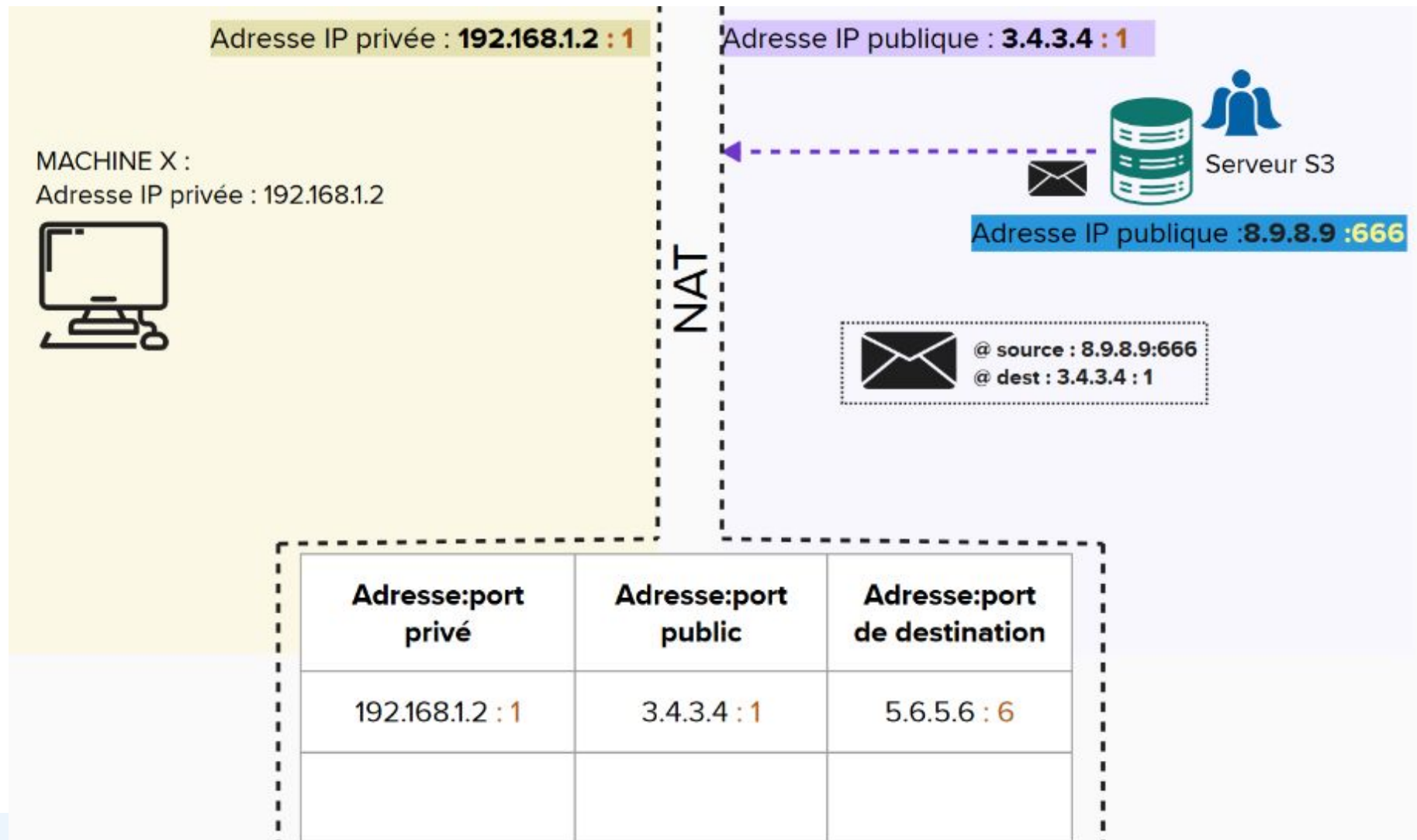
Problèmes engendrés, ou sécurité ?



Problèmes engendrés, ou sécurité ?



Problèmes engendrés, ou sécurité ?



Méthodes de franchissement :

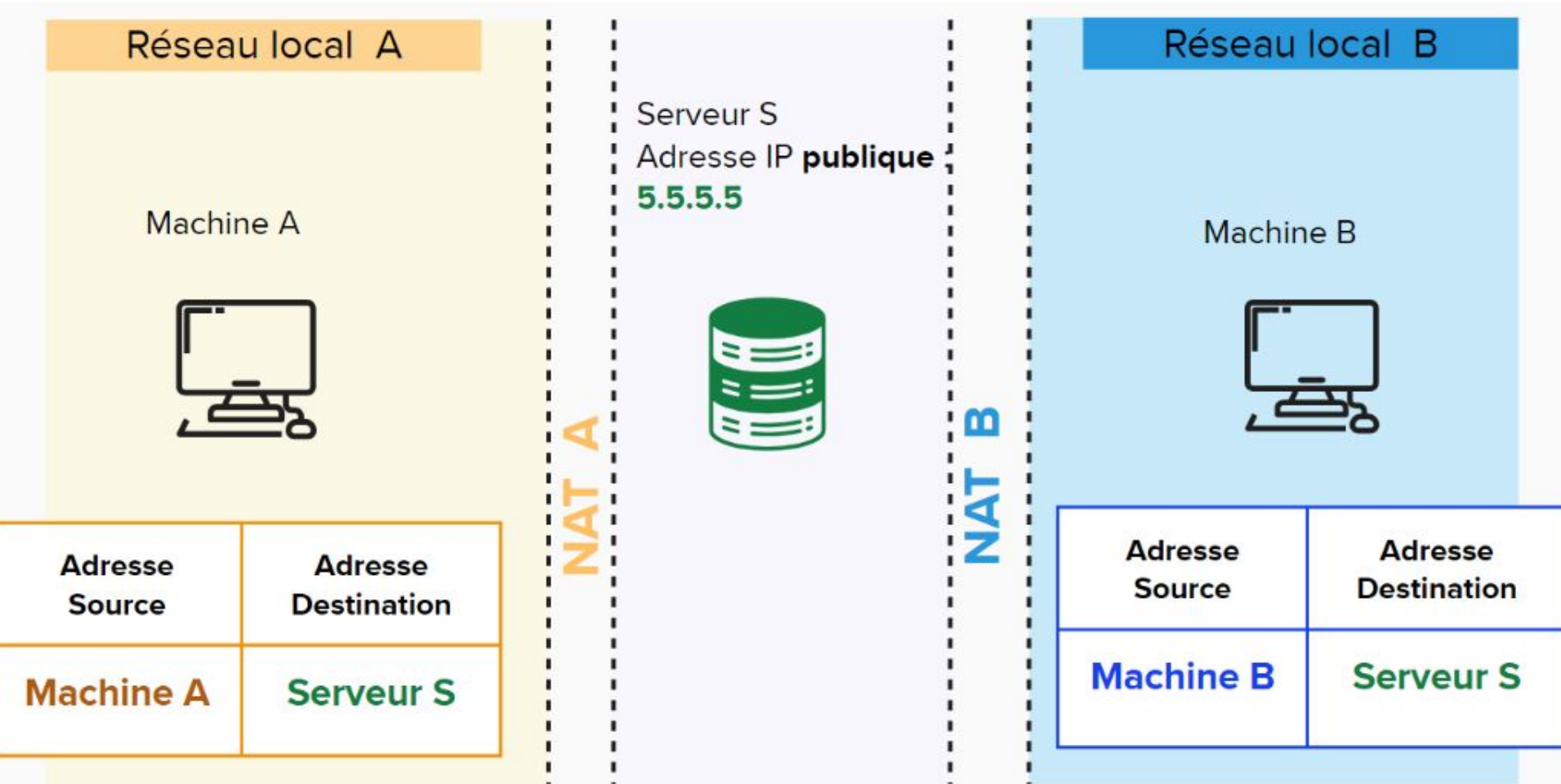
2 méthodes de franchissement :

1. Le Relaying
2. Le Hole Punching

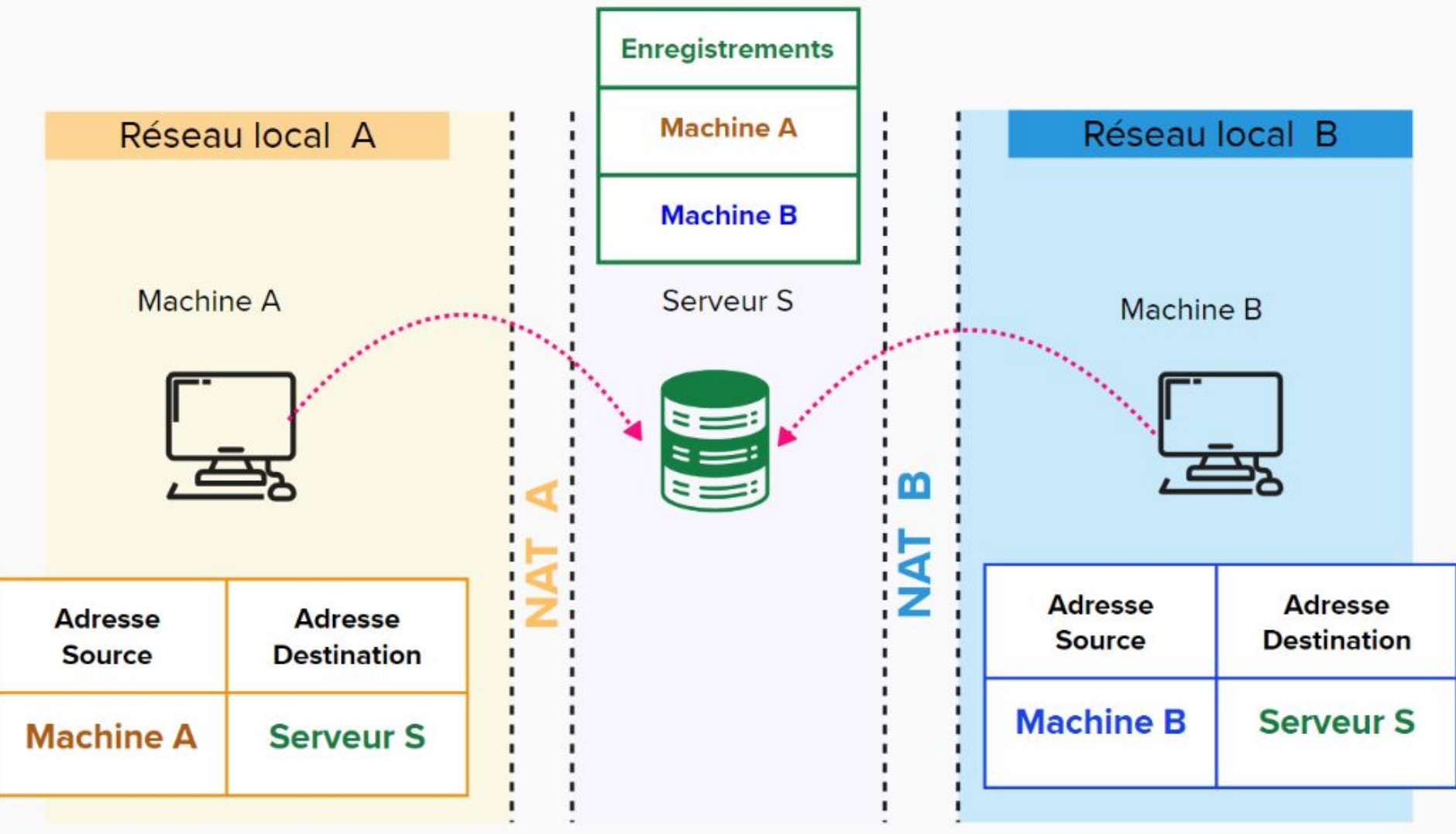
→ Les NAT ne sont pas infranchissables

RFC 5128 : State of Peer-to-Peer (P2P) Communication across NATs

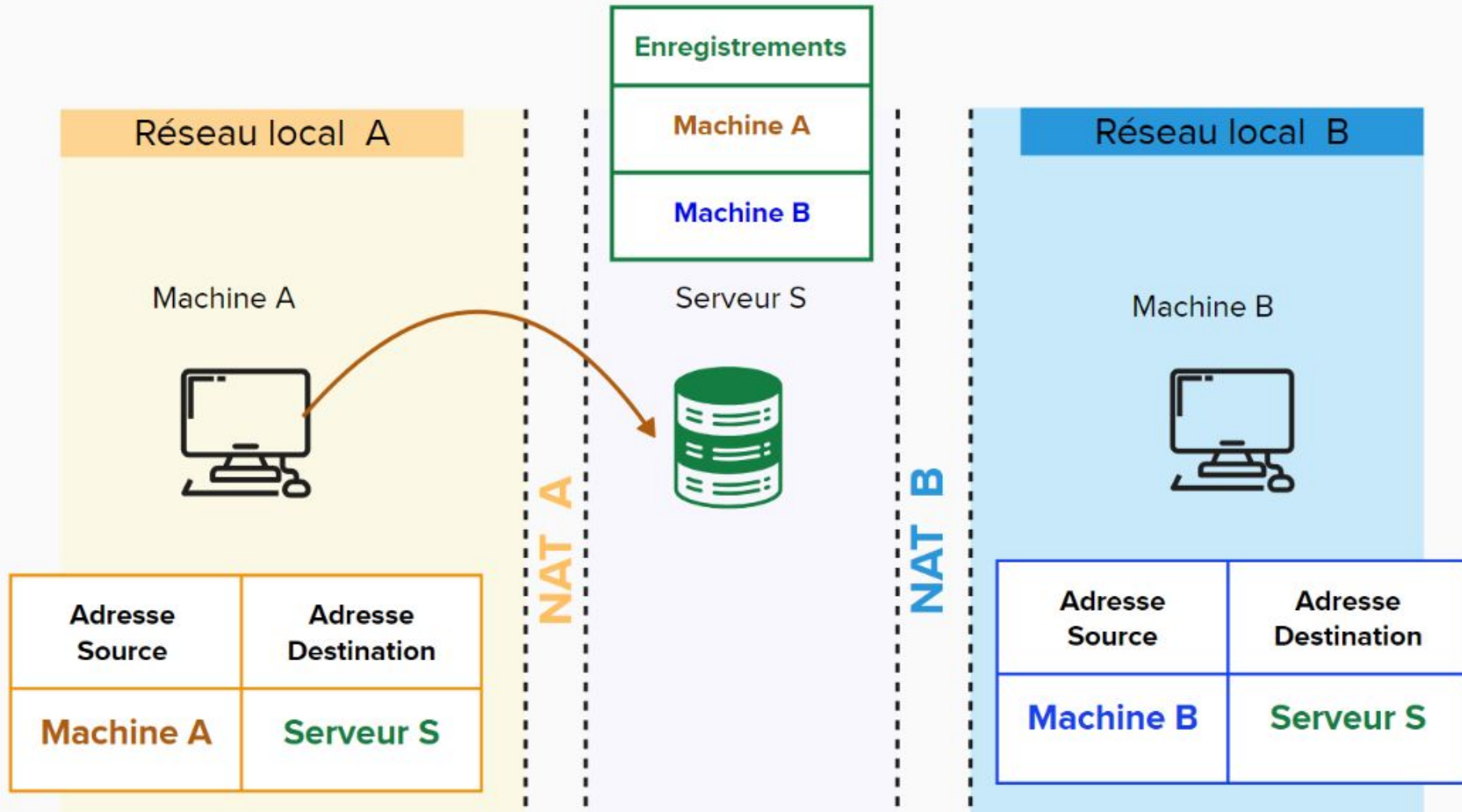
Méthodes de franchissement : Relaying



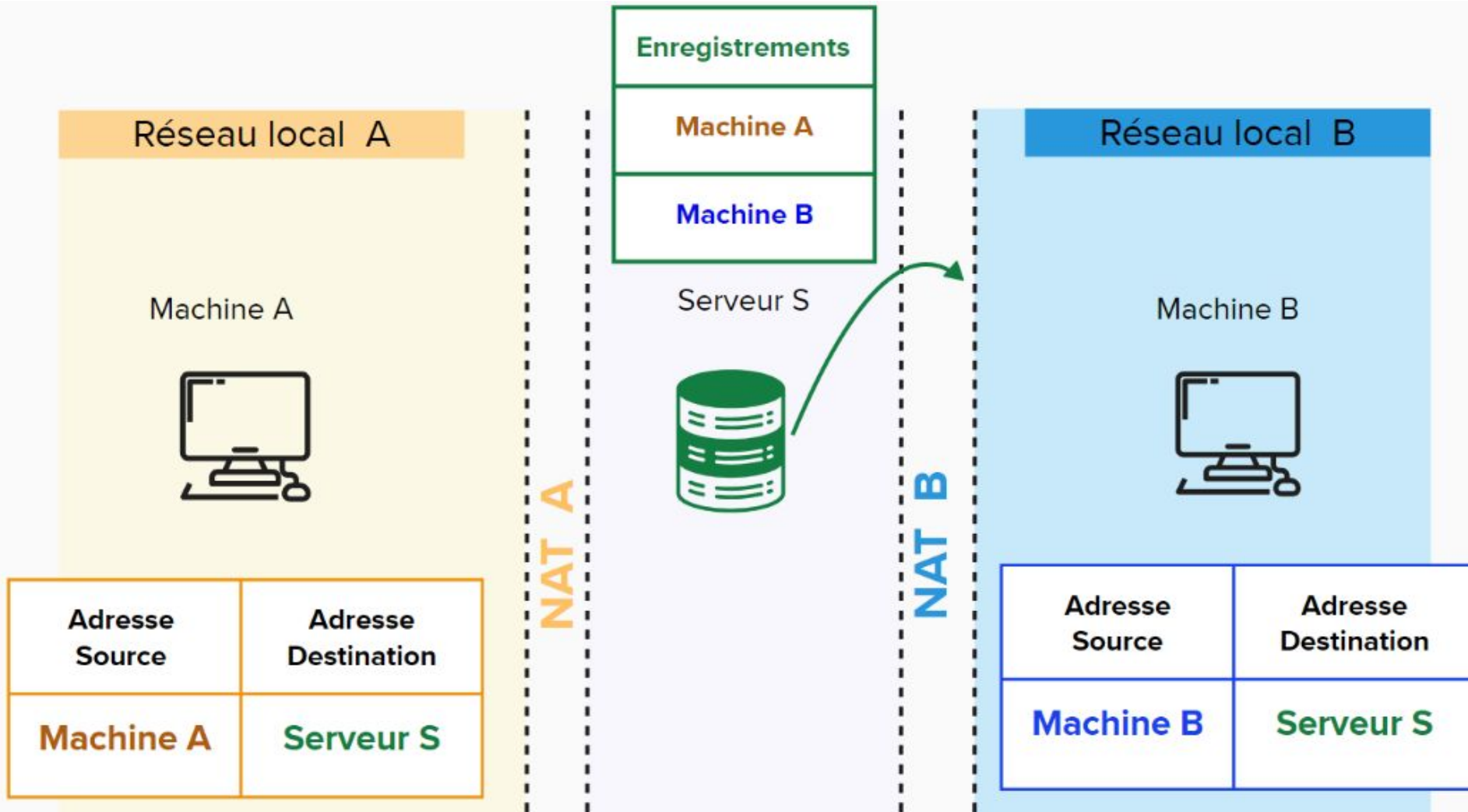
Méthodes de franchissement : Relaying



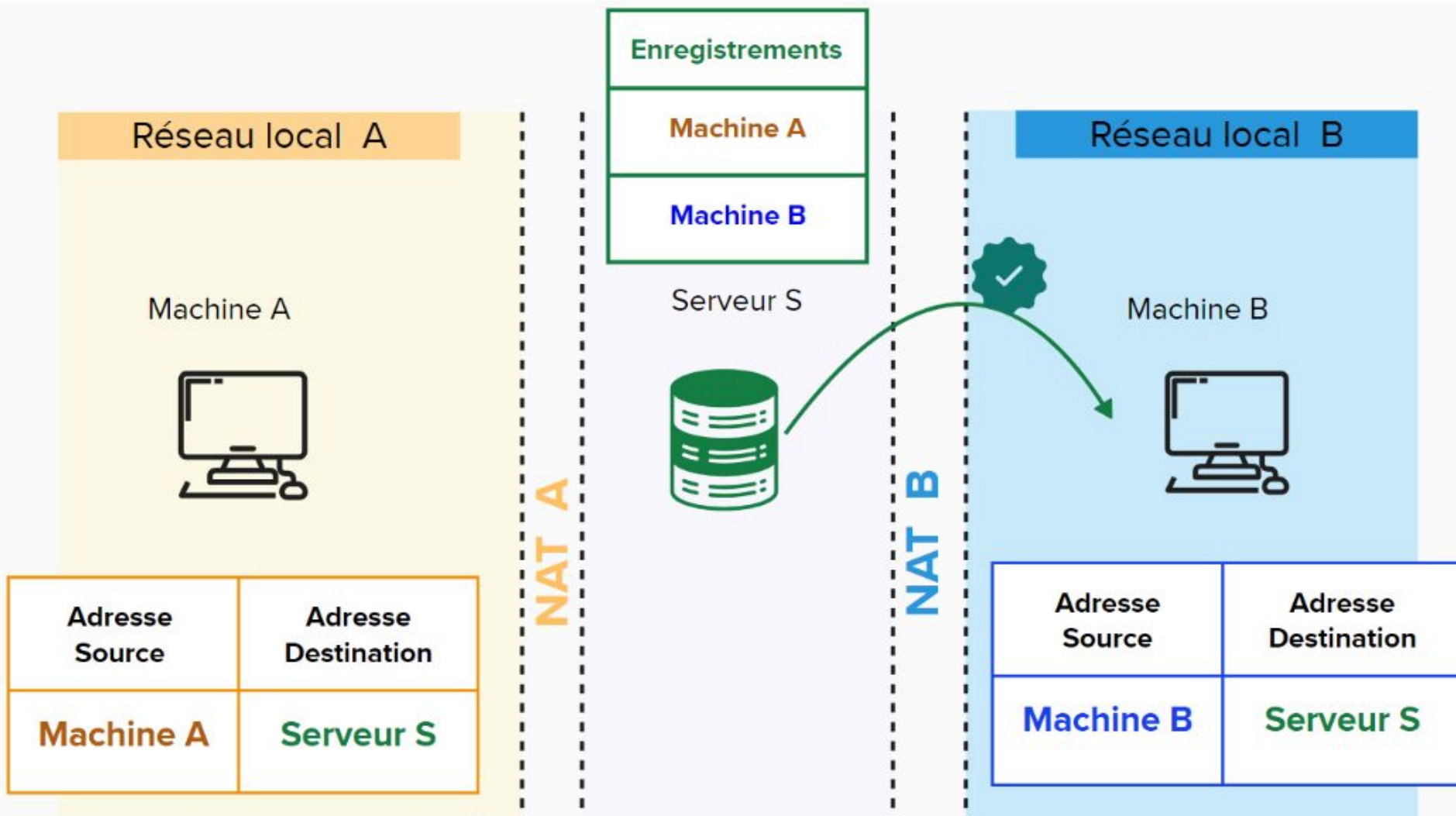
Méthodes de franchissement : Relaying



Méthodes de franchissement : Relaying



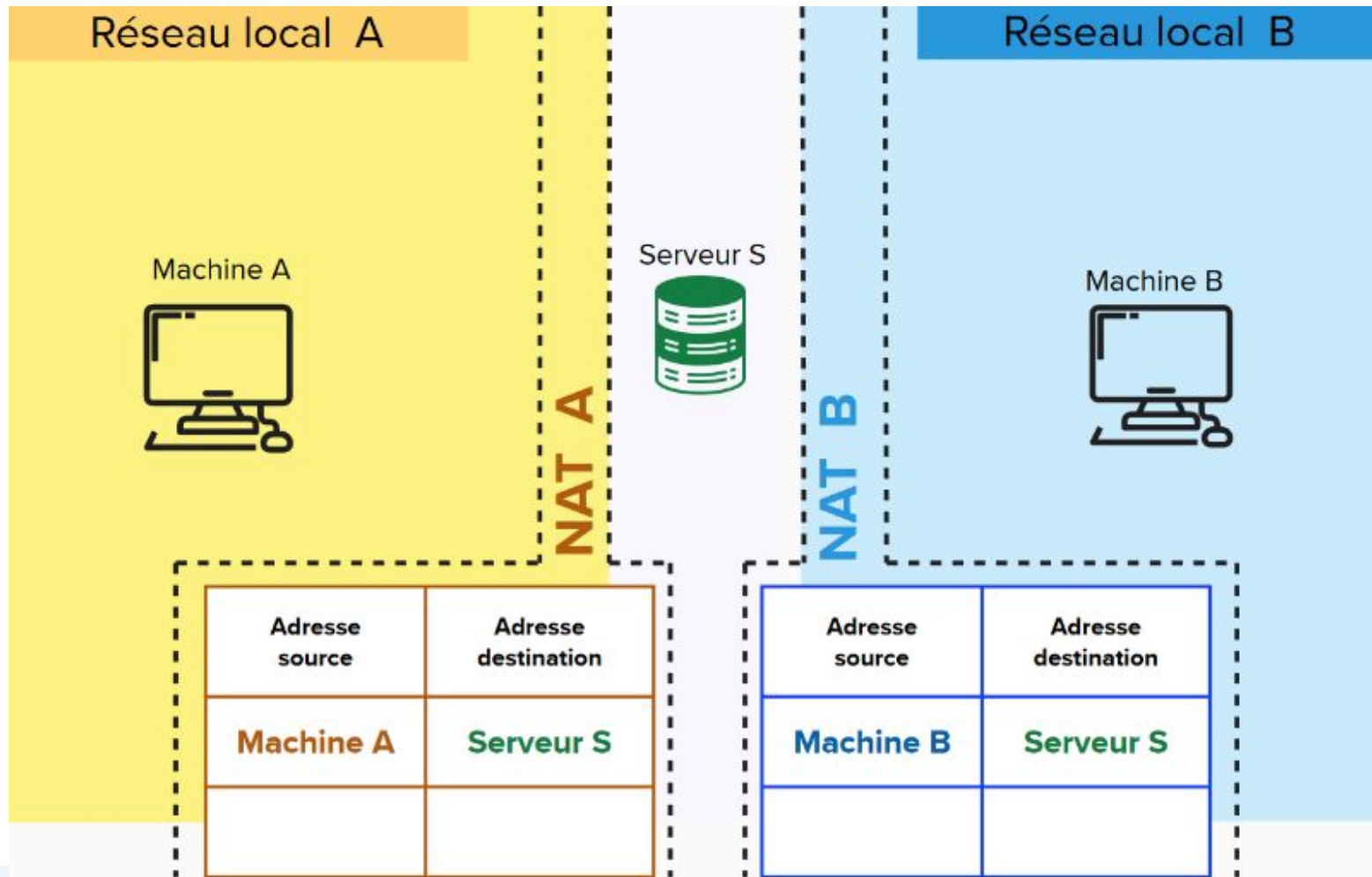
Méthodes de franchissement : Relaying



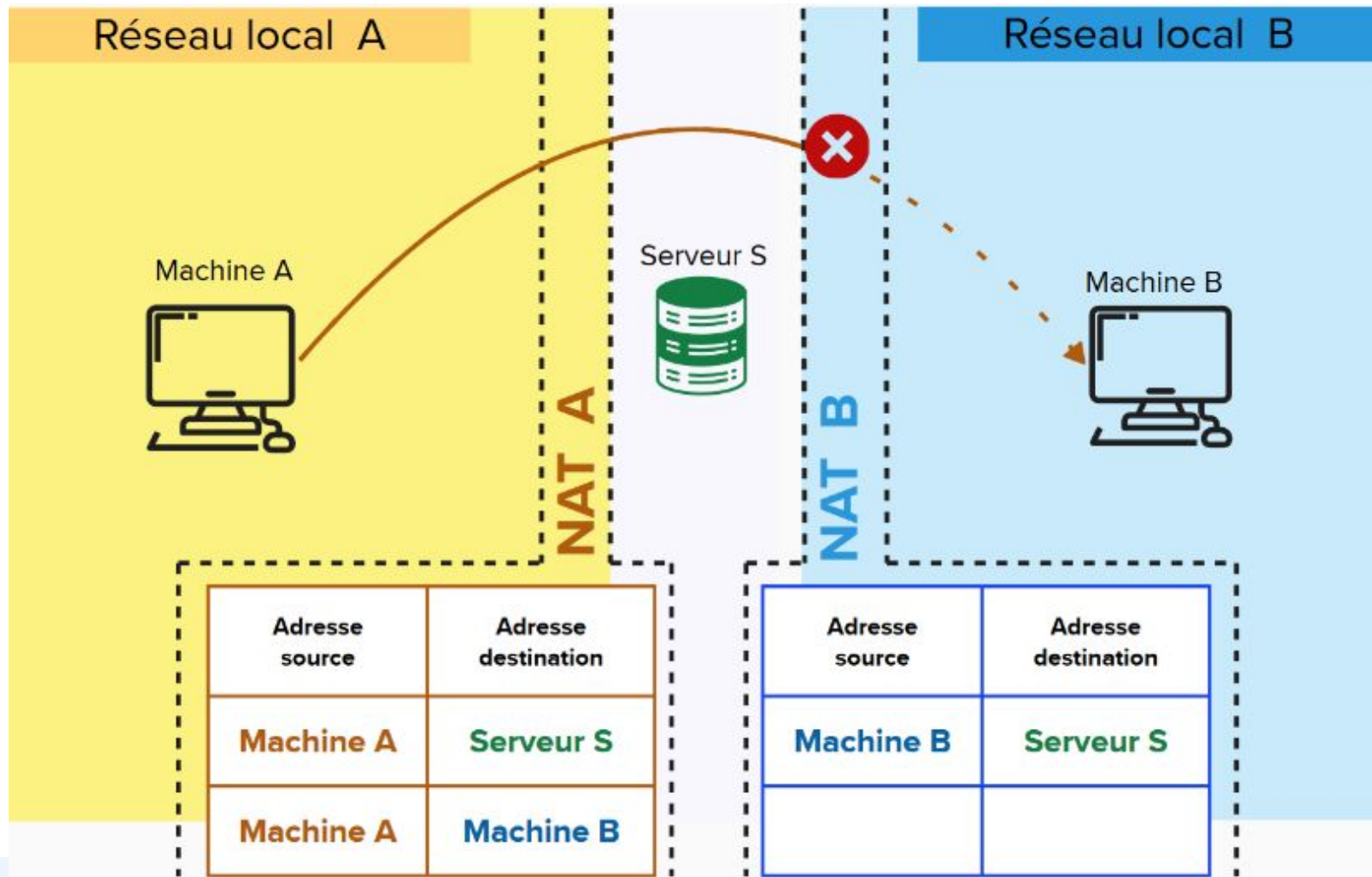
Méthodes de franchissement : Relaying

- **Avantage du Relaying** : Fonctionne avec tous les types de NAT
- **Inconvénients** : Passer par un serveur intermédiaire est coûteux en ressources matérielles

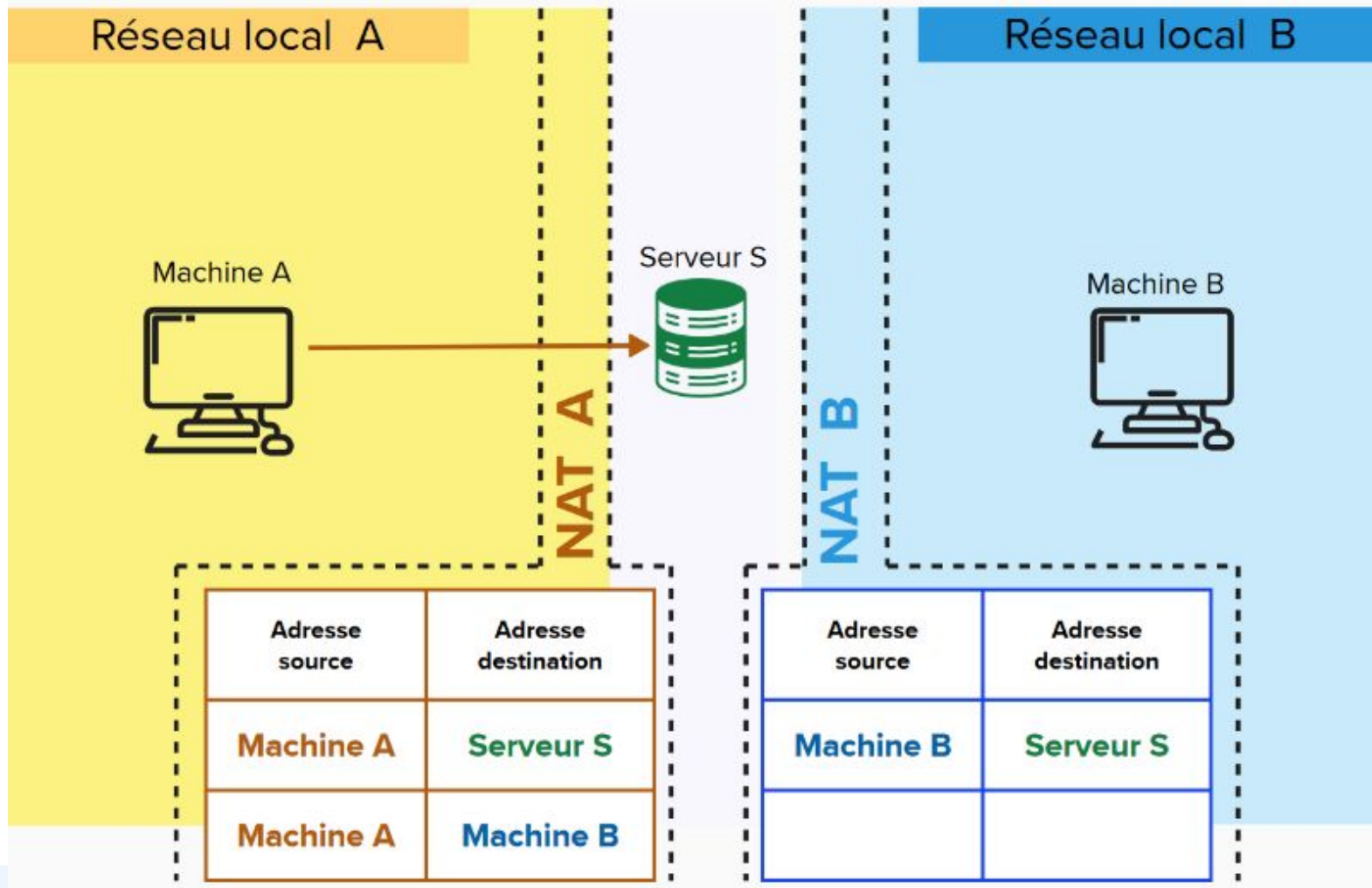
Méthodes de franchissement : Hole Punching



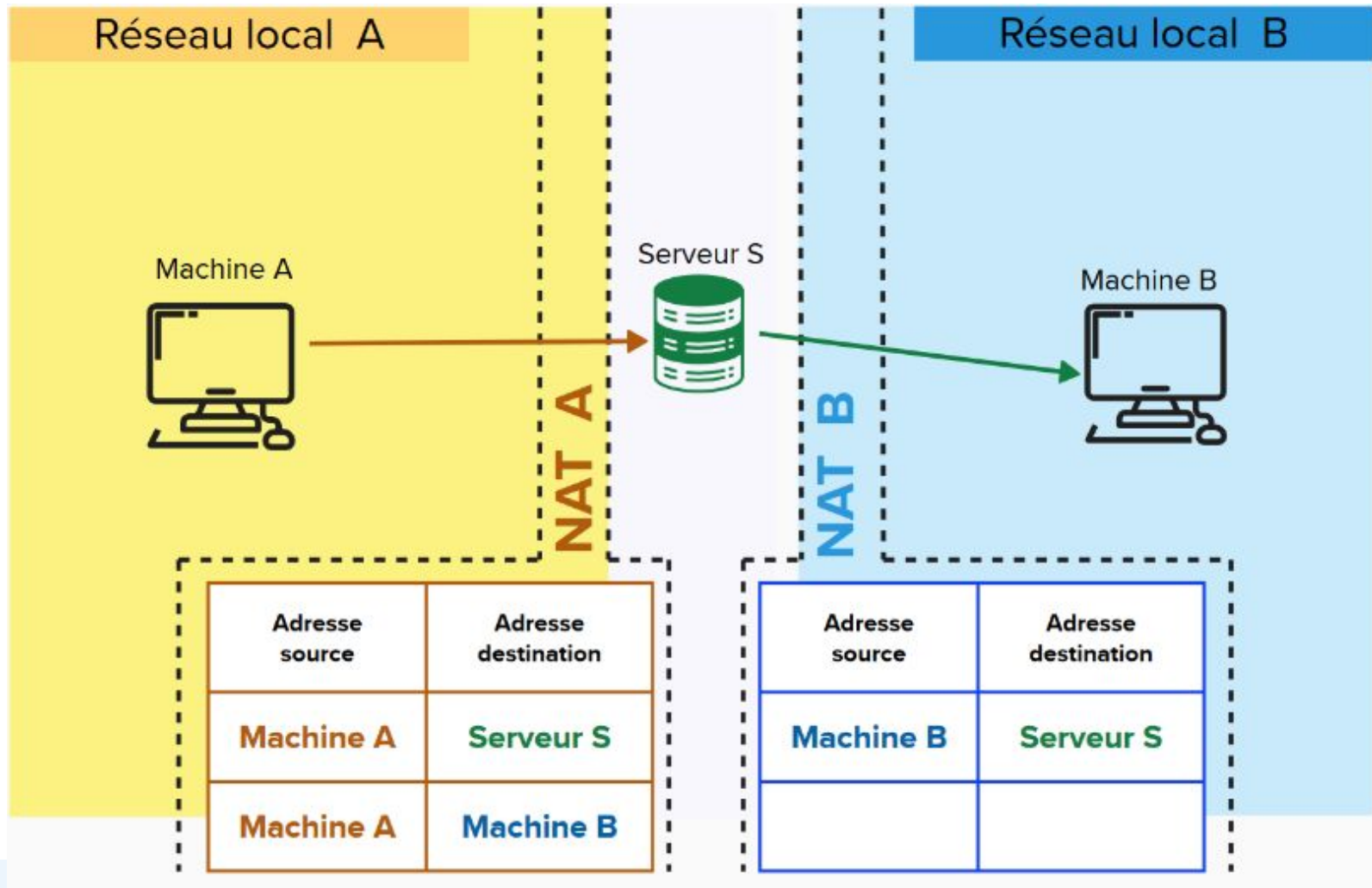
Méthodes de franchissement : Hole Punching



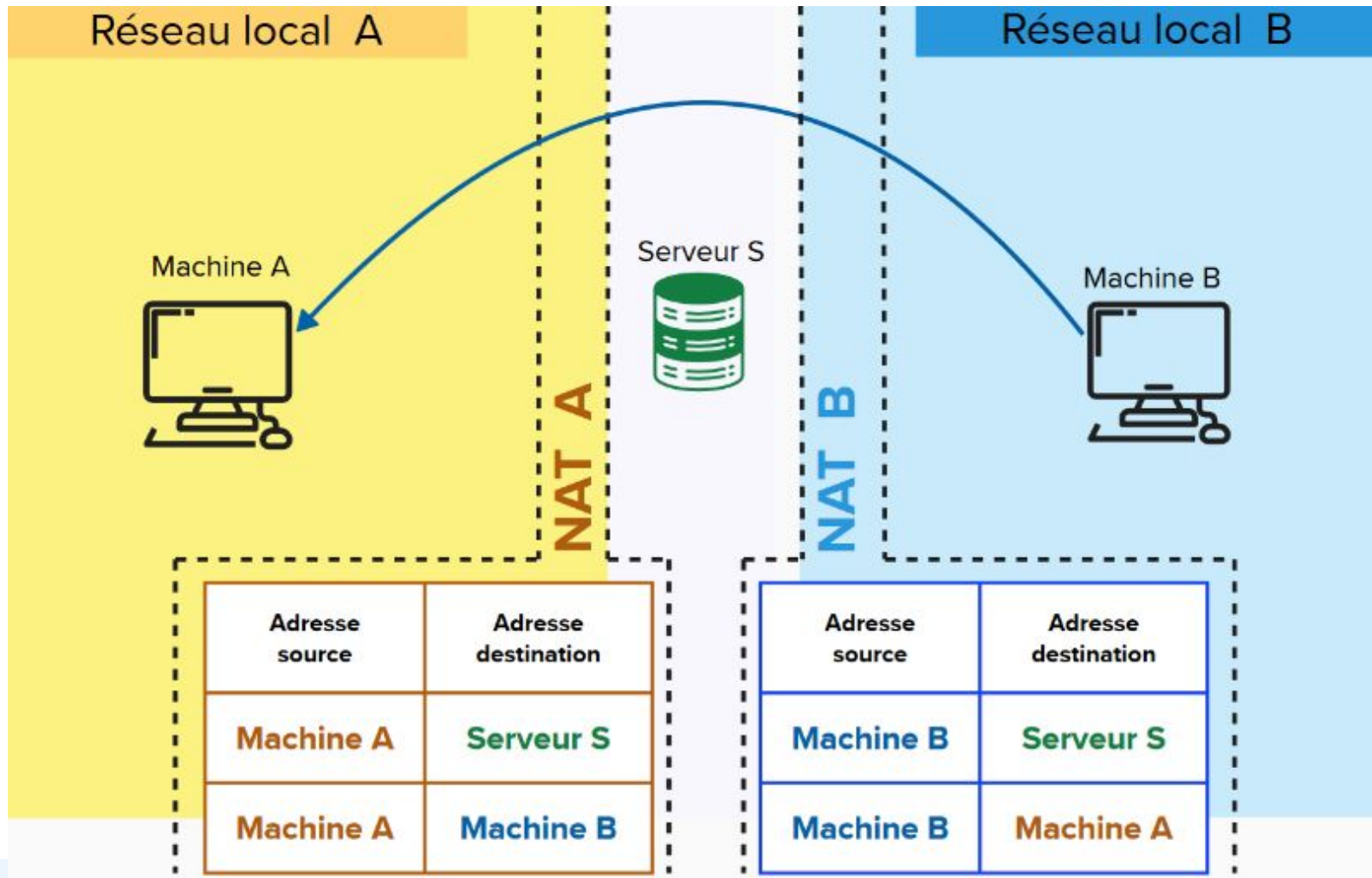
Méthodes de franchissement : Hole Punching



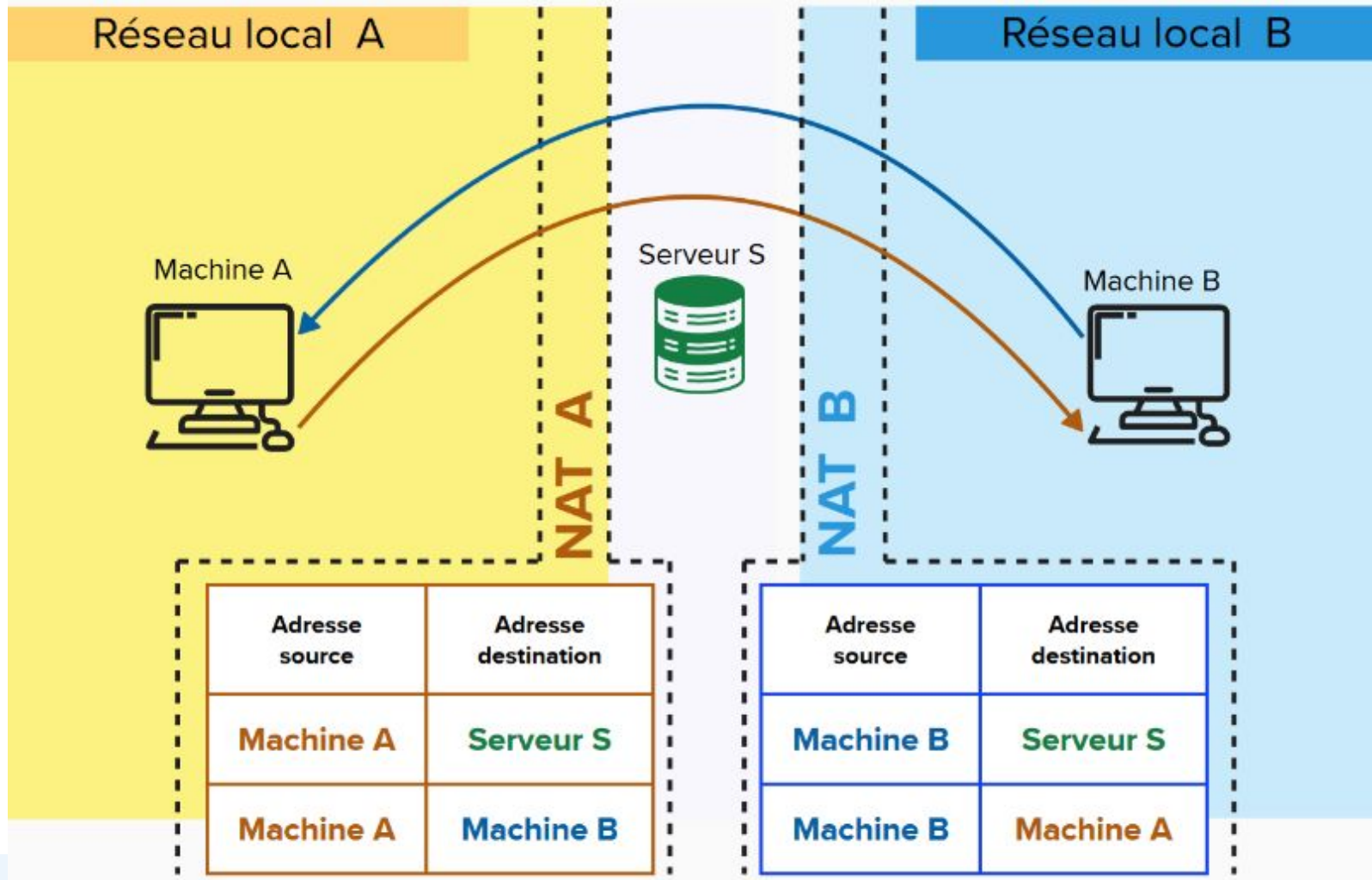
Méthodes de franchissement : Hole Punching



Méthodes de franchissement : Hole Punching



Méthodes de franchissement : Hole Punching



Méthodes de contournement : Hole Punching

- **Avantage du Hole Punching** : Communication directe entre les hôtes sans passer par S
- **Inconvénient** : Réitérer le processus à chaque changement de port/d'adresse source

Méthodes de contournement : ICE

- **Protocole ICE (Interactive Connectivity Establishment) : RFC 8445**
 - Implémentation concrète

Méthodes de contournement : ICE

- **Protocole ICE (Interactive Connectivity Establishment) : RFC 8445**
 - Implémentation concrète
- Priorisation du Hole Punching avant de passer au Relaying

Méthodes de contournement : ICE

- **Protocole ICE (Interactive Connectivity Establishment) : RFC 8445**
 - Implémentation concrète
- Priorisation du Hole Punching avant de passer au Relaying
- Autres fonctionnalités

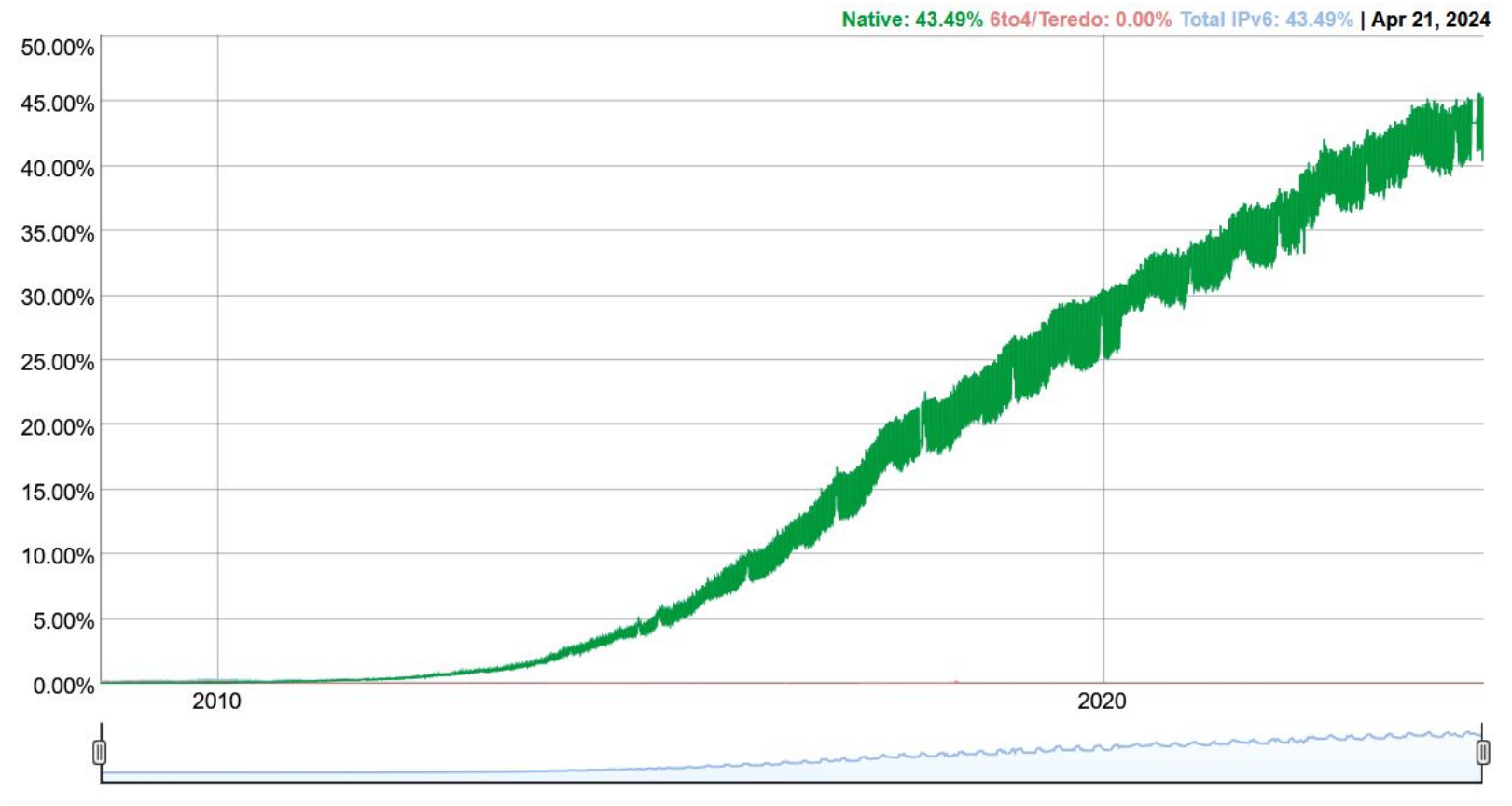
Le futur des NAT

- Plusieurs options possibles :
 - On reste dans le *statu quo* actuel : un manque d'adresses IPv4

Le futur des NAT

- Plusieurs options possibles :
 - On reste dans le *statu quo* actuel : un manque d'adresses IPv4
 - Passage à IPv6

Le futur des NAT



Adoption d'IPv6 parmi les utilisateurs des services de Google

Le futur des NAT

- Plusieurs options possibles :
 - On reste dans le *statu quo* actuel : un manque d'adresses IPv4
 - Passage à IPv6
 - Entre-deux : utilisation de méthodes d'interconnexions

Conclusion : Les NAT sont-ils infranchissables ?

- Les NAT : traducteurs d'adresses
 - Effets secondaires
 - Sécurité ?
 - Problèmes
- ⇒ Ils deviennent des barrières, qui peuvent être franchies
- Plus besoin de NAT en IPv6

Conclusion : Les NAT sont-ils infranchissables ?

Perceptions communes des NAT et documentation

- Livres
 - Les NAT : des dispositifs sécuritaires ?
- RFC - Articles - Normes ISO

Bibliographie

- [1] Brian E. Carpenter. Internet Transparency. Request for Comments RFC 2775. Num Pages : 18. Internet Engineering Task Force, fév. 2000. doi : 10.17487/RFC2775. url : <https://datatracker.ietf.org/doc/rfc2775> (visité le 19/05/2024).
- [2] José Dordoigne. Réseaux informatiques Notions fondamentales (9e édition) - (Protocoles, Architectures, Réseaux sans fil...) Editions ENI, 2022. 804 pages. isbn : 978-2-409-03517-3.
- [3] Kjeld Borch Egevang et Paul Francis. The IP Network Address Translator (NAT). Request for Comments RFC 1631. Num Pages : 10. Internet Engineering Task Force, mai 1994. doi : 10.17487/RFC1631. url : <https://datatracker.ietf.org/doc/rfc1631> (visité le 29/03/2024).
- [4] Kjeld Borch Egevang et Pyda Srisuresh. Traditional IP Network Address Translator (Traditional NAT). Request for Comments RFC 3022. Num Pages : 16. Internet Engineering Task Force, jan. 2001. doi : 10.17487/RFC3022. url : <https://datatracker.ietf.org/doc/rfc3022> (visité le 29/03/2024).
- [5] Bryan Ford, Dan Kegel et Pyda Srisuresh. State of Peer-to-Peer (P2P) Communication across Network Address Translators (NATs). Request for Comments RFC 5128. Num Pages : 32. Internet Engineering Task Force, mars 2008. doi : 10.17487/RFC5128. url : <https://datatracker.ietf.org/doc/rfc5128> (visité le 29/03/2024).

Bibliographie

[6] Bryan Ford et al. NAT Behavioral Requirements for TCP. Request for Comments RFC 5382. Num Pages : 31. Internet Engineering Task Force, oct. 2008. doi : 10.17487/RFC5382. url : <https://datatracker.ietf.org/doc/rfc5382> (visité le 29/03/2024).

[7] Saikat Guha et al. NAT Behavioral Requirements for ICMP. Request for Comments RFC 5508. Num Pages : 29. Internet Engineering Task Force, avr. 2009. doi : 10.17487/RFC5508. url : <https://datatracker.ietf.org/doc/rfc5508> (visité le 29/03/2024).

[8] Christer Holmberg et Justin Uberti. Interactive Connectivity Establishment Patiently Awaiting Connectivity (ICE PAC). Request for Comments RFC 8863. Num Pages : 6. Internet Engineering Task Force, jan. 2021. doi : 10.17487/RFC8863. url : <https://datatracker.ietf.org/doc/rfc8863> (visité le 03/04/2024).

[9] IPv6 – Google. url : <https://www.google.fr/ipv6/statistics.html#tab=ipv6-adoption> (visité le 23/04/2024).

[10] IPv6 – Google. IPv6 – Google. url : <https://www.google.fr/ipv6/statistics.html#tab=ipv6-adoption> (visité le 23/04/2024).

[11] Cullen Fluffy Jennings et Francois Audet. Network Address Translation (NAT) Behavioral Requirements for Unicast UDP. Request for Comments RFC 4787. Num Pages : 29. Internet Engineering Task Force, jan. 2007. doi : 10.17487/RFC4787. url : <https://datatracker.ietf.org/doc/rfc4787> (visité le 29/03/2024).

Bibliographie

[12] Orestis Kanaris et Johan Pouwelse. Mass Adoption of NATs : Survey and experiments on carriergrade NATs. 15 nov. 2023. arXiv : 2311.04658[cs]. url : <http://arxiv.org/abs/2311.04658> (visit  le 29/03/2024).

[13] Ari Ker nen, Christer Holmberg et Jonathan Rosenberg. Interactive Connectivity Establishment (ICE) : A Protocol for Network Address Translator (NAT) Traversal. Request for Comments RFC 8445. Num Pages : 100. Internet Engineering Task Force, juill. 2018. doi : 10.17487/RFC8445. url : <https://datatracker.ietf.org/doc/rfc8445> (visit  le 03/04/2024).

[14] Ioana Livadariu et al. “Inferring Carrier-Grade NAT Deployment in the Wild”. In : IEEE INFOCOM 2018 - IEEE Conference on Computer Communications. IEEE INFOCOM 2018 - IEEE Conference on Computer Communications. Avr. 2018, p. 2249-2257. doi : 10.1109/INFOCOM.2018.8486223. url : <https://ieeexplore.ieee.org/document/8486223> (visit  le 29/03/2024).

[15] Philip Matthews, Jonathan Rosenberg et Rohan Mahy. Traversal Using Relays around NAT (TURN) : Relay Extensions to Session Traversal Utilities for NAT (STUN). Request for Comments RFC 5766. Num Pages : 67. Internet Engineering Task Force, avr. 2010. doi : 10.17487/RFC5766. url : <https://datatracker.ietf.org/doc/rfc5766> (visit  le 03/04/2024).

Bibliographie

- [16] Christian JACQUENET Mohamed BOUCADAIR. Contrôle dynamique de ressources Internet. Techniques de l'Ingénieur. 10 nov. 2014. url : <https://www-techniques-ingenieur-fr.scd-rproxy.u-strasbg.fr/base-documentaire/technologies-de-l-information-th9/administration-de-reseaux-applications-et-mise-en-oeuvre-42481210/contrôle-dynamique-de-ressources-internet-te7612/> (visité le 29/03/2024).
- [17] Robert Moskowitz et al. Address Allocation for Private Internets. Request for Comments RFC 1918. Num Pages : 9. Internet Engineering Task Force, fév. 1996. doi : 10.17487/RFC1918. url : <https://datatracker.ietf.org/doc/rfc1918> (visité le 29/03/2024).
- [18] Notice détaillée norme. Sécurité de l'information, cybersécurité et protection de la vie privée - Systèmes de management de la sécurité de l'information - Exigences. Juill. 2023. url : <https://cobazafnor-org.scd-rproxy.u-strasbg.fr/notice/norme/nf-en-iso-iec-27001/FA206487?rechercheID=22800293&searchIndex=1&activeTab=all> (visité le 17/04/2024).
- [19] Reinaldo Penno et al. Updates to Network Address Translation (NAT) Behavioral Requirements. Request for Comments RFC 7857. Num Pages : 14. Internet Engineering Task Force, avr. 2016. doi : 10.17487/RFC7857. url : <https://datatracker.ietf.org/doc/rfc7857> (visité le 29/03/2024).
- [20] Simon Perreault et al. Common Requirements for Carrier-Grade NATs (CGNs). Request for Comments RFC 6888. Num Pages : 15. Internet Engineering Task Force, avr. 2013. doi : 10.17487/RFC6888. url : <https://datatracker.ietf.org/doc/rfc6888> (visité le 29/03/2024).

Bibliographie

[21] Tirumaleswar Reddy.K et al. Traversal Using Relays around NAT (TURN) : Relay Extensions to Session Traversal Utilities for NAT (STUN). Request for Comments RFC 8656. Num Pages : 79. Internet Engineering Task Force, fév. 2020. doi : 10.17487/RFC8656. url : <https://datatracker.ietf.org/doc/rfc8656> (visité le 19/05/2024).

[22] RIPE NCC IPv4 Pool. RIPE NCC IPv4 Pool. url : <https://www.ripe.net/manage-ips-and-asns/ipv4/ipv4-pool/> (visité le 23/04/2024).

[23] Jonathan Rosenberg et al. STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs). Request for Comments RFC 3489. Num Pages : 47. Internet Engineering Task Force, mars 2003. doi : 10.17487/RFC3489. url : <https://datatracker.ietf.org/doc/rfc3489> (visité le 03/04/2024).

[24] Jonathan Rosenberg et al. TCP Candidates with Interactive Connectivity Establishment (ICE). Request for Comments RFC 6544. Num Pages : 29. Internet Engineering Task Force, mars 2012. doi : 10.17487/RFC6544. url : <https://datatracker.ietf.org/doc/rfc6544> (visité le 03/04/2024).

[25] Claude Servin. Réseaux & télécoms. 4e éd. DUNOD. 800 p. isbn : 978-2-10-059258-6.

[26] Transmission Control Protocol. Request for Comments RFC 793. Num Pages : 91. Internet Engineering Task Force, sept. 1981. doi : 10.17487/RFC0793. url : <https://datatracker.ietf.org/doc/rfc793> (visité le 29/03/2024).