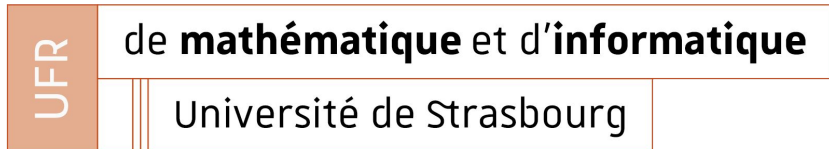


# Les NAT sont-ils infranchissables ?

L2S4 PRDS



Par Carine Wakim & Maxime Zingraff, 27.03.2024

# Le remplissage manuel

**TP-LINK**

**TL-ER6120**

**NAT Setup** | One-to-One NAT | Multi-Nets NAT | Virtual Server | Port Triggering | ALG

**One-to-One NAT**

Mapping IP Address: 192.168.0.3 -> 123.1.1.3

Interface: WAN1

DMZ Forwarding: ☒ Enable ☐ Disable

Description: WEB (Optional)

Status: ☒ Activate ☐ Inactivate

**List of Rules**

No.	Original IP	Translated IP	Interface	DMZ Forwarding	Description	Status	Action
No entries.							

Select All | Activate | Inactivate | Delete | Search

**Callouts:**

- Enter private IP (points to Mapping IP Address)
- Enter public IP (points to Translated IP)
- Click on Add (points to Add button)
- Select Enable (points to Enable radio button)
- Select Activate (points to Activate radio button)

TP-Link, "How to configure One-to-One NAT on Safestream routers using the old GUI",  
<https://www.tp-link.com/us/support/faq/381/>

# Les méthodes de remplissage des tables de traduction

2 méthodes :

1. Remplissage manuel
2. Remplissage automatique  
(*ex : contournement des NAT*)

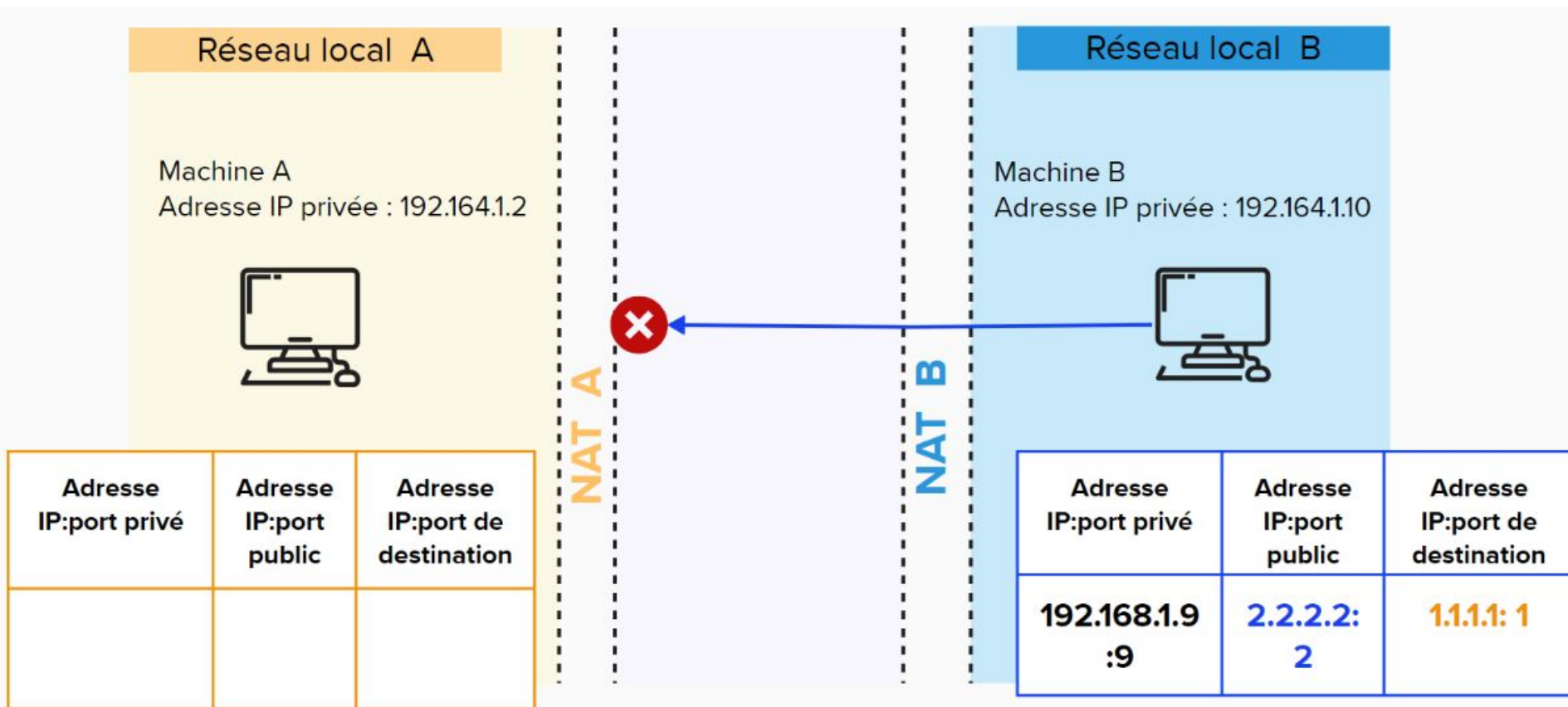
→ Aujourd'hui : Quelles sont les différentes méthodes pour contourner les NAT ?

# Les méthodes de contournement des NAT

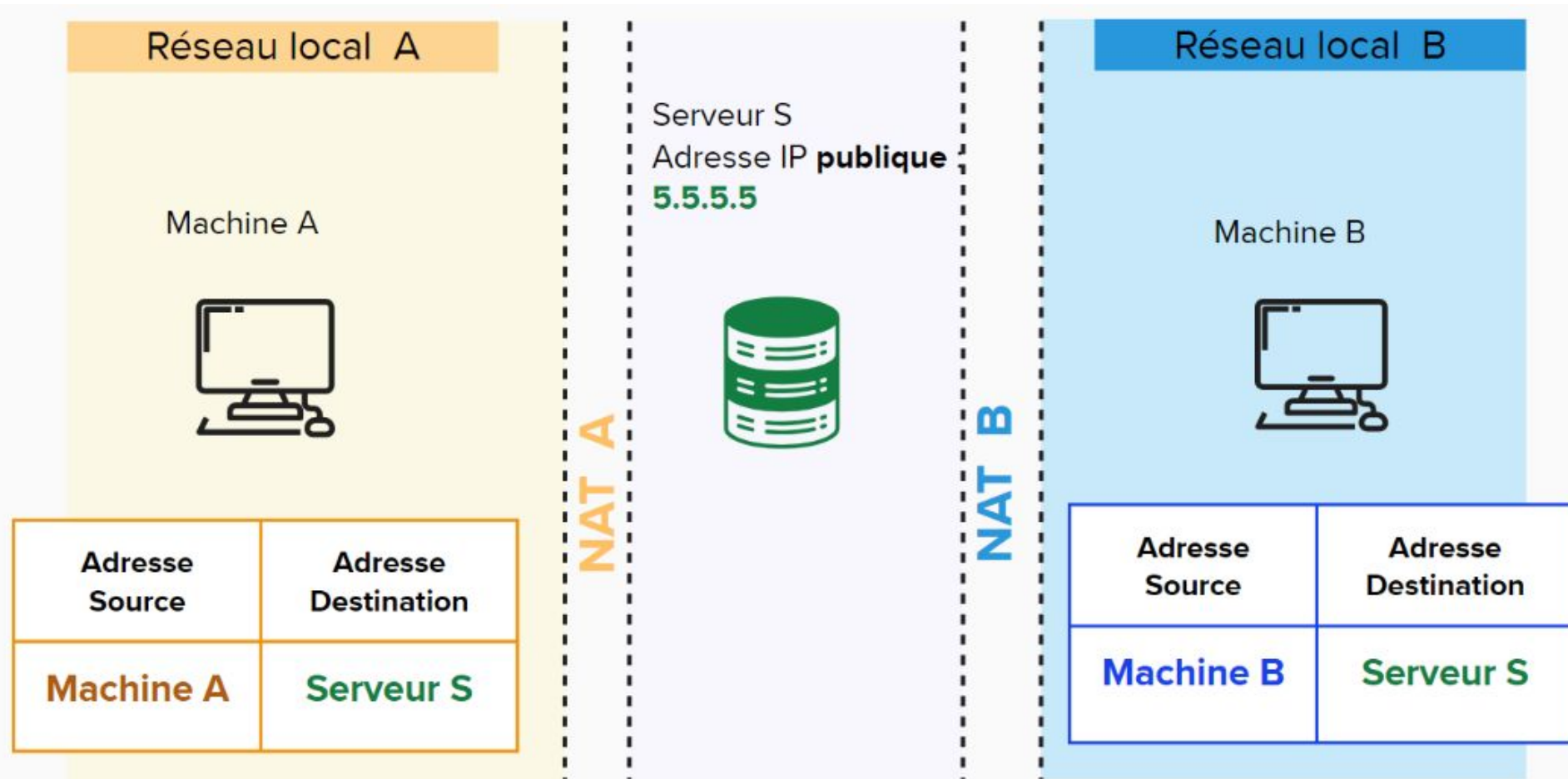
3 méthodes de contournement :

1. Relaying (Relais)
2. Connection Reversal
3. Hole Punching

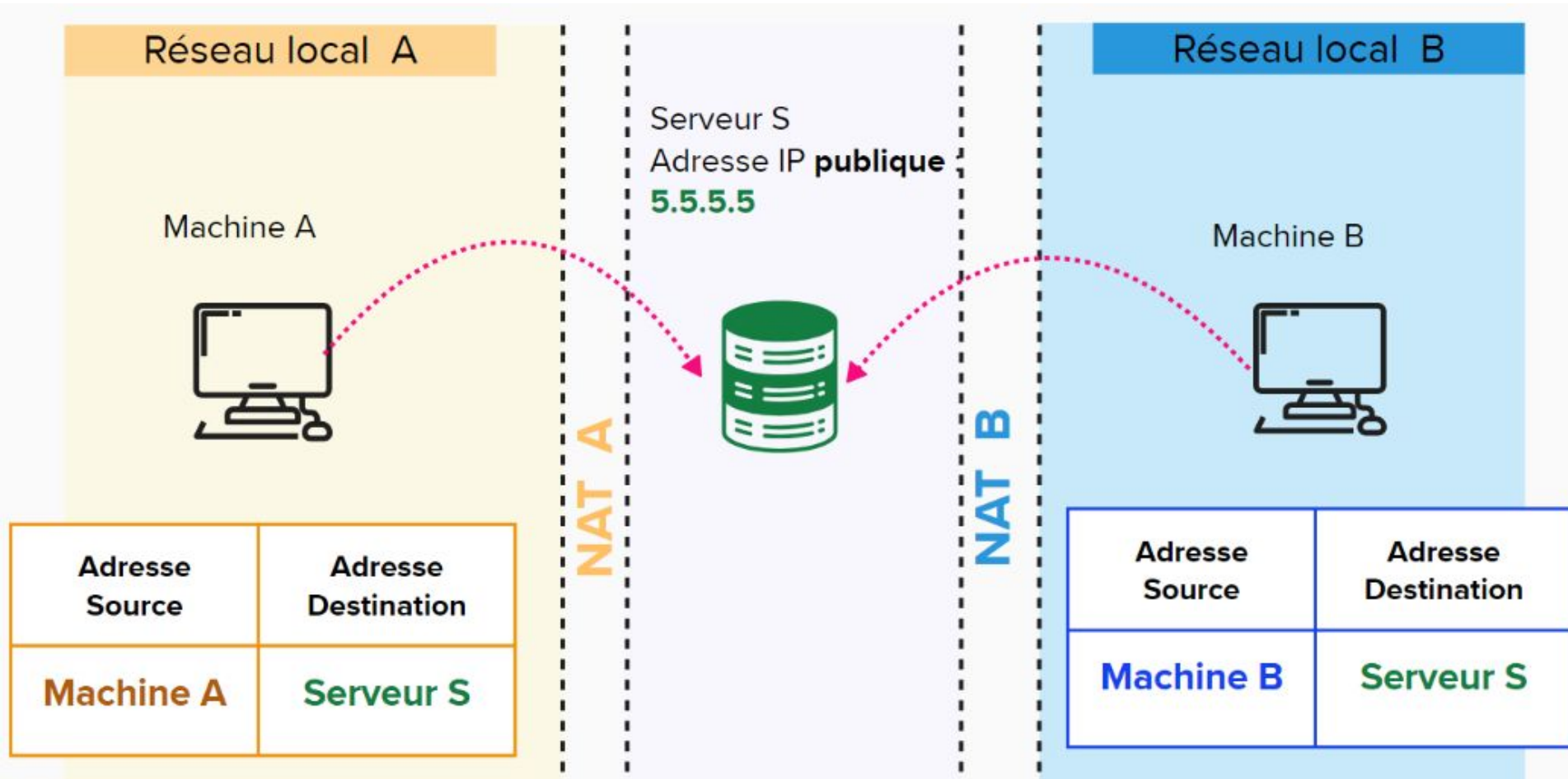
# Relaying



# Relaying

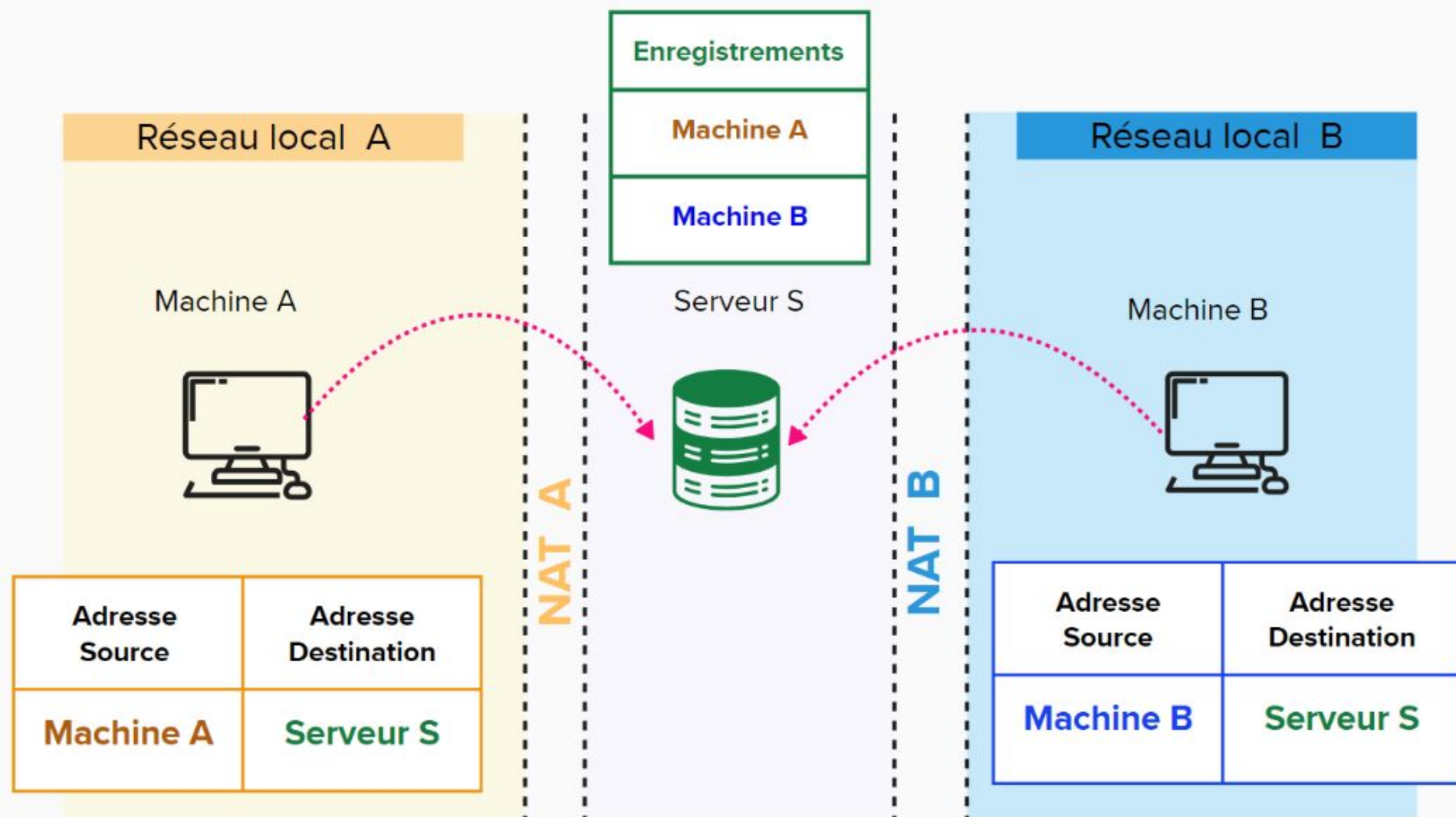


# Relaying : Enregistrement auprès du serveur



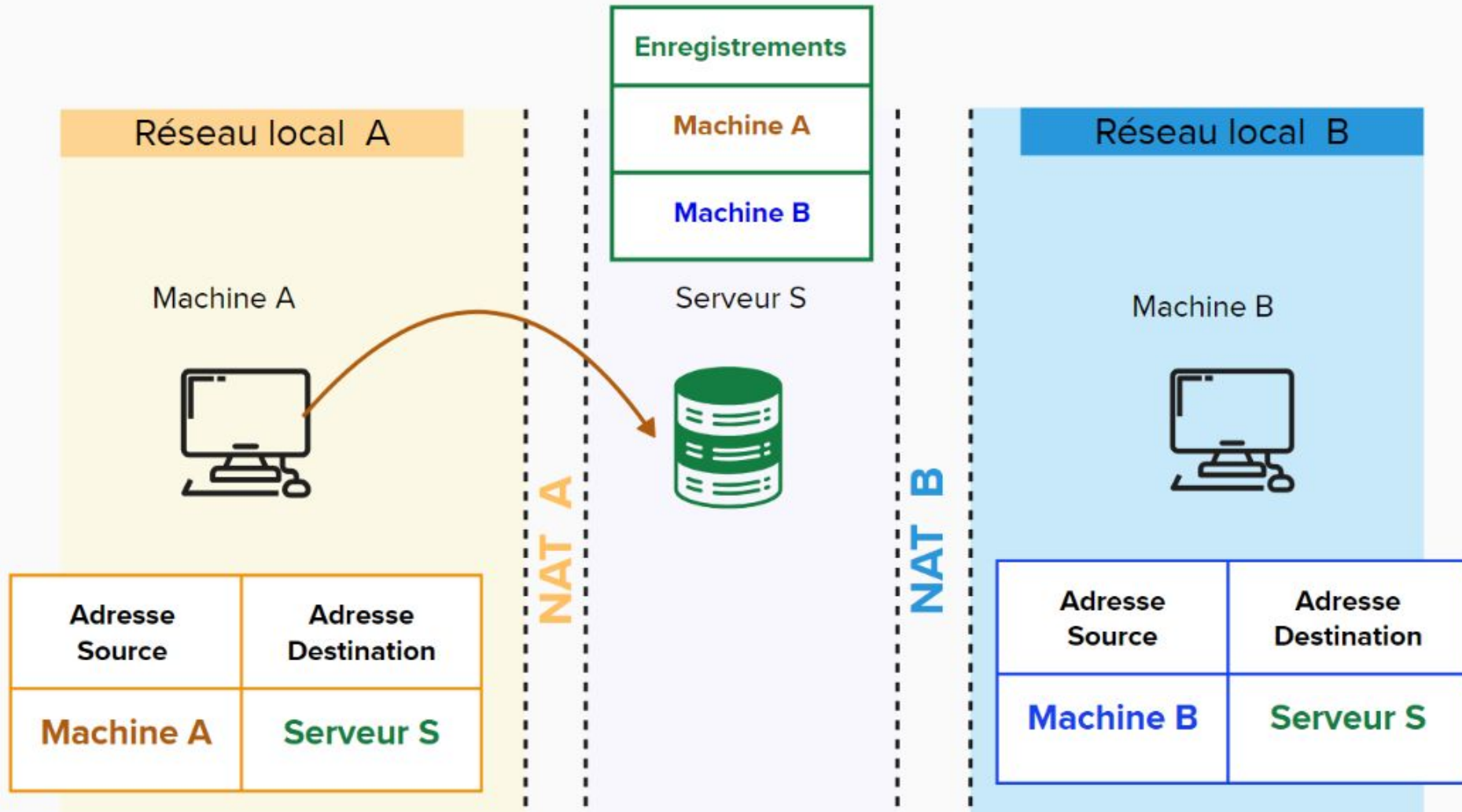


# Relaying : Enregistrement auprès du serveur

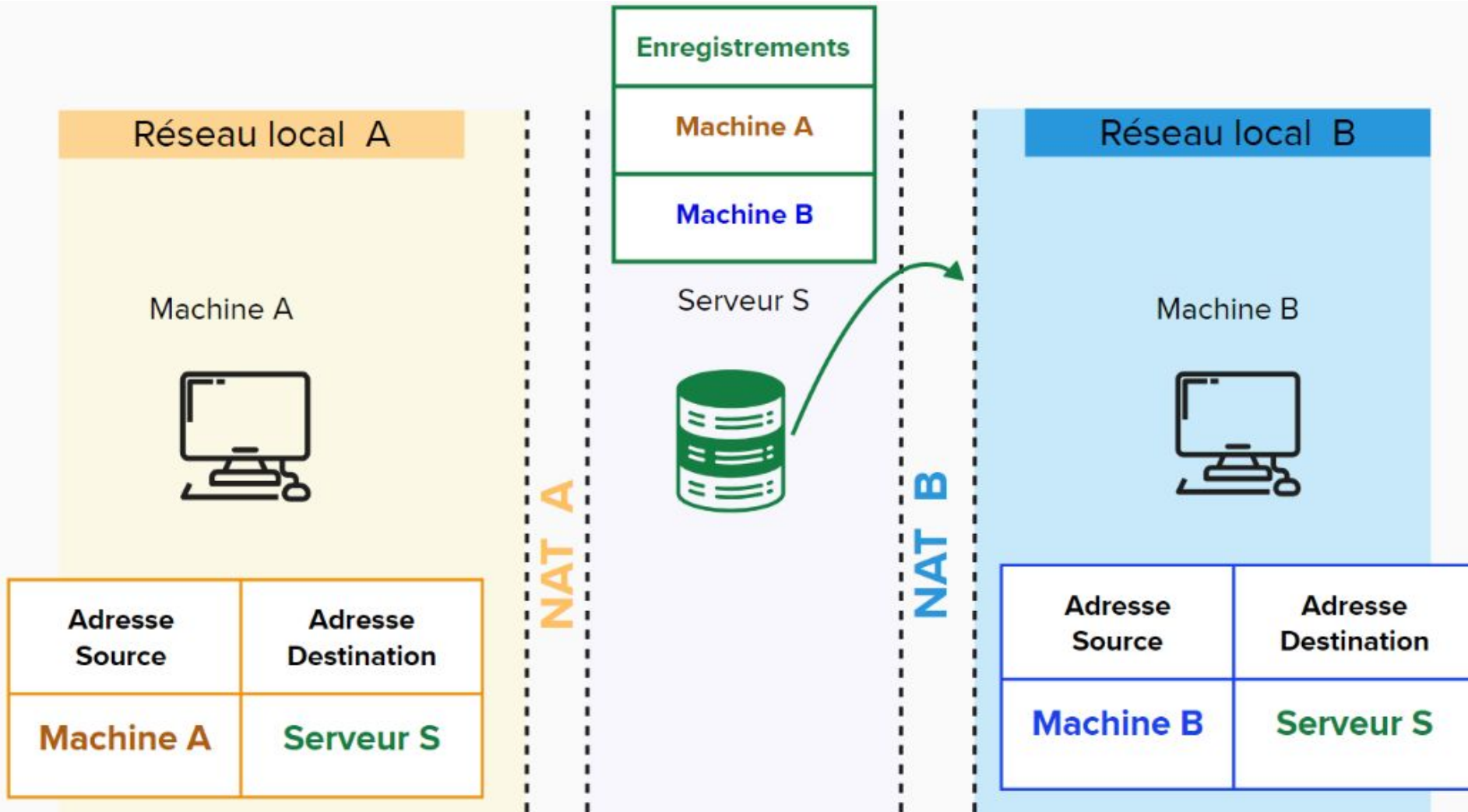




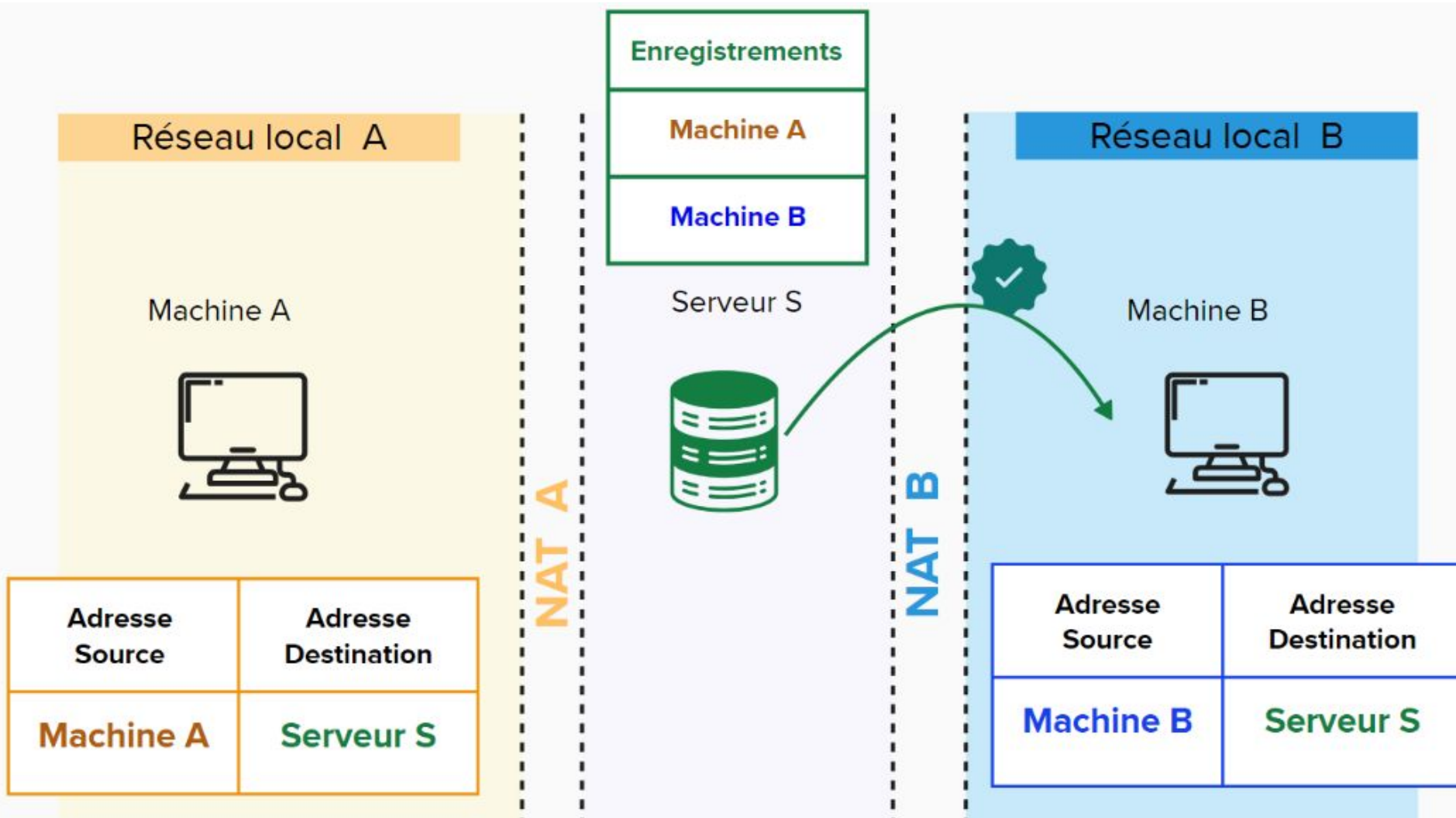
# Relaying : Établissement de la communication



# Relaying : Établissement de la communication



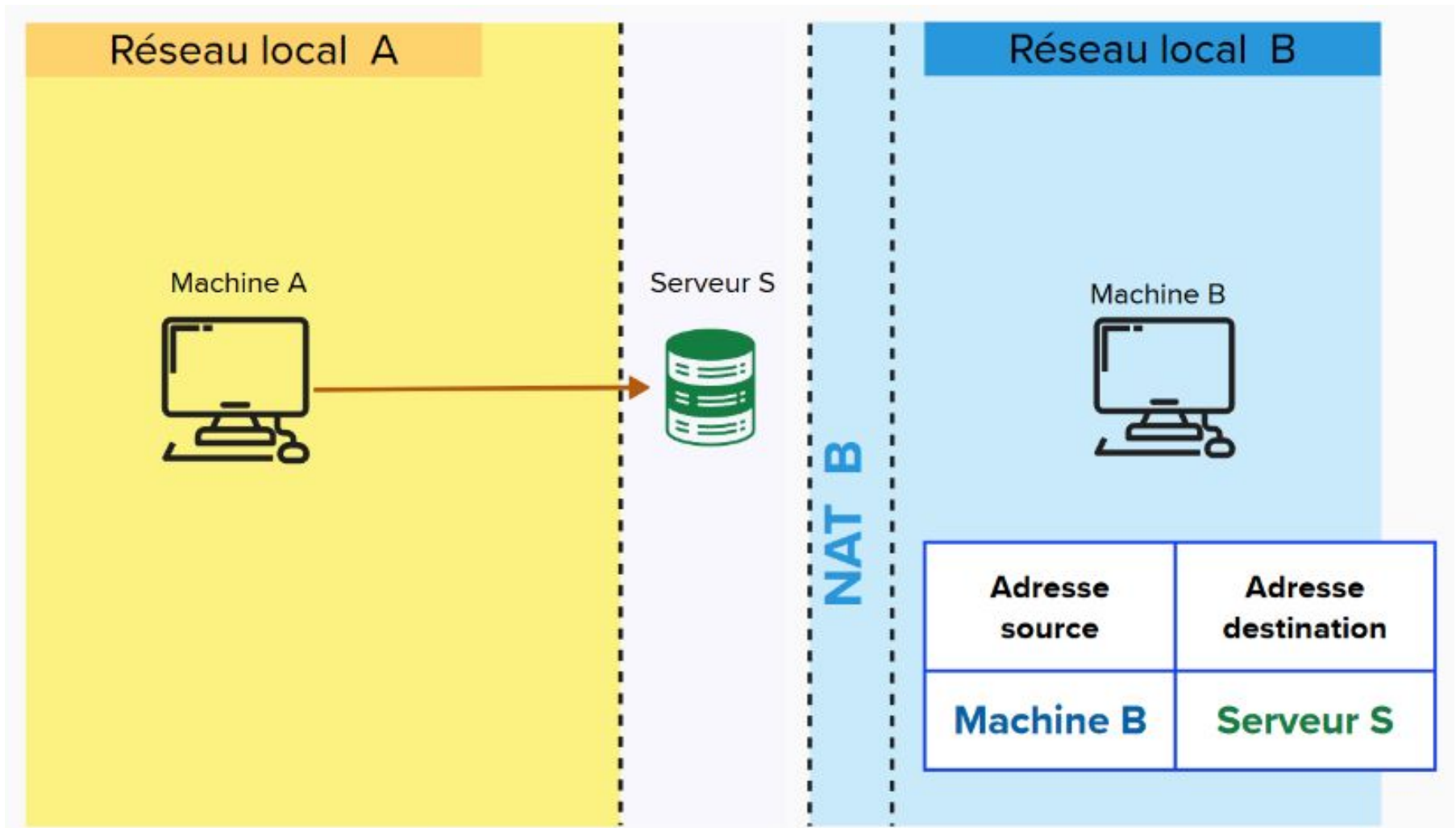
# Relaying : Établissement de la communication



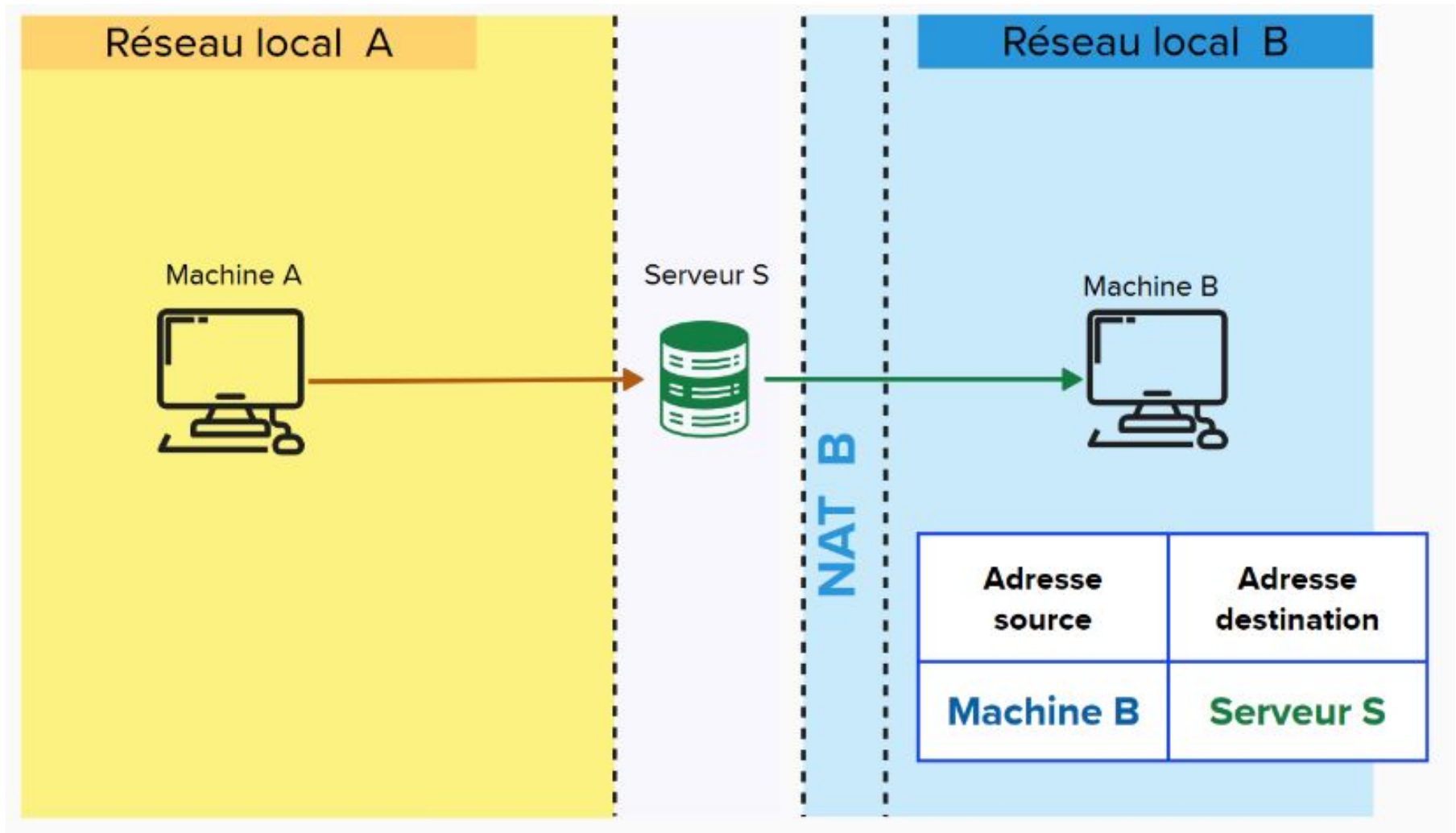
# Relaying : Avantage et inconvénient

- Avantage :
  - Fonctionne avec tous les types de NAT
- Inconvénient :
  - Très coûteux

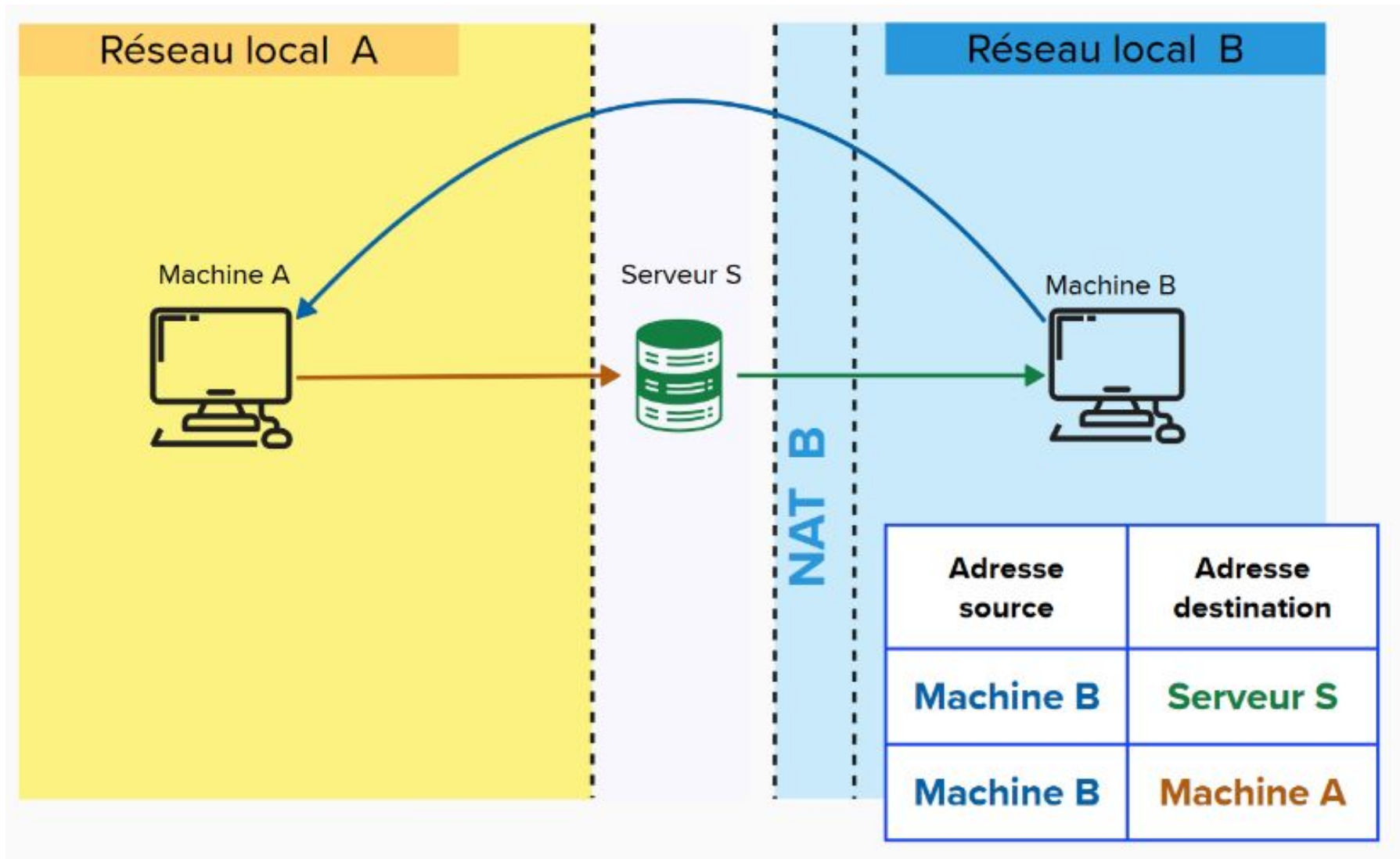
# Connexion Reversal



# Connexion Reversal

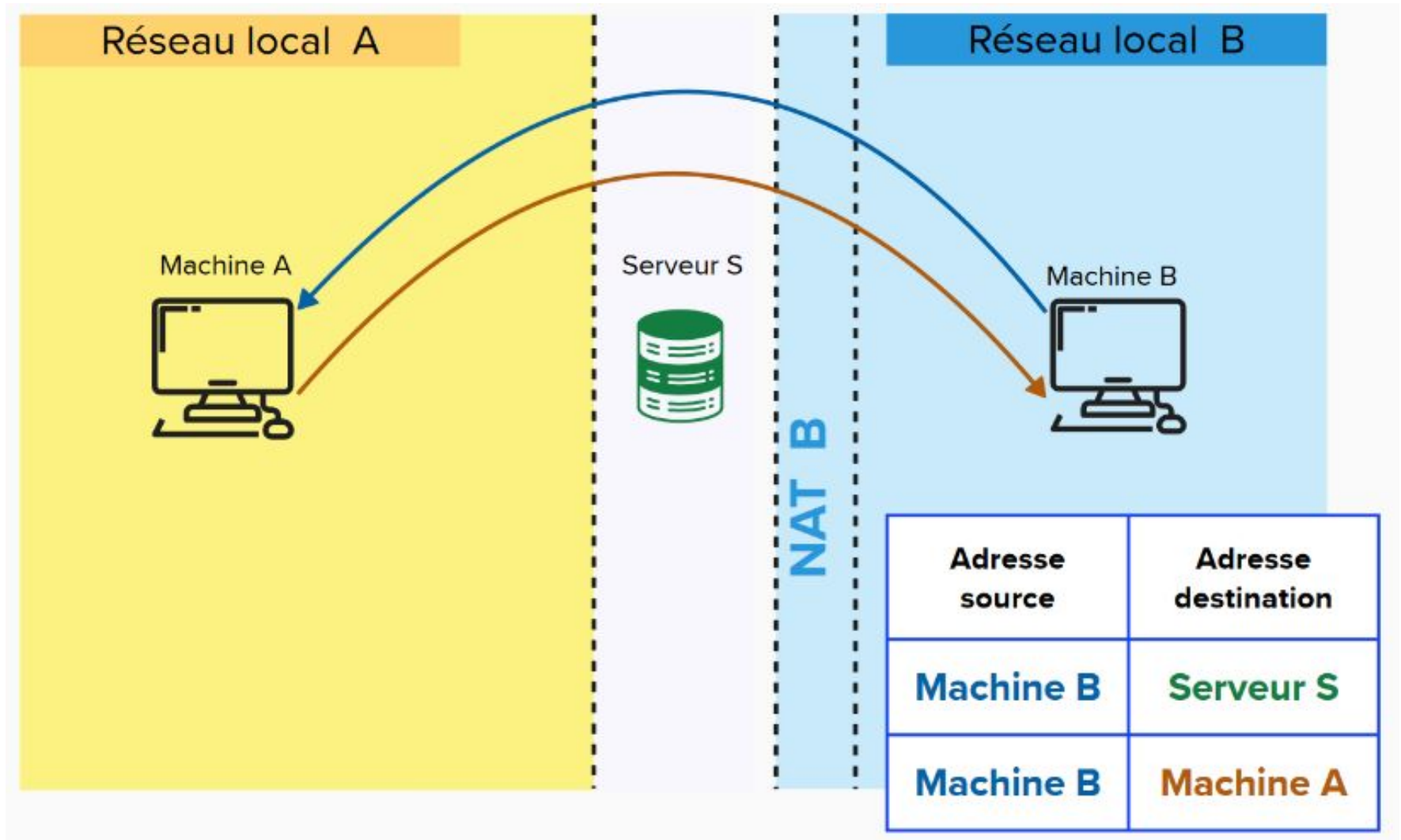


# Connexion Reversal





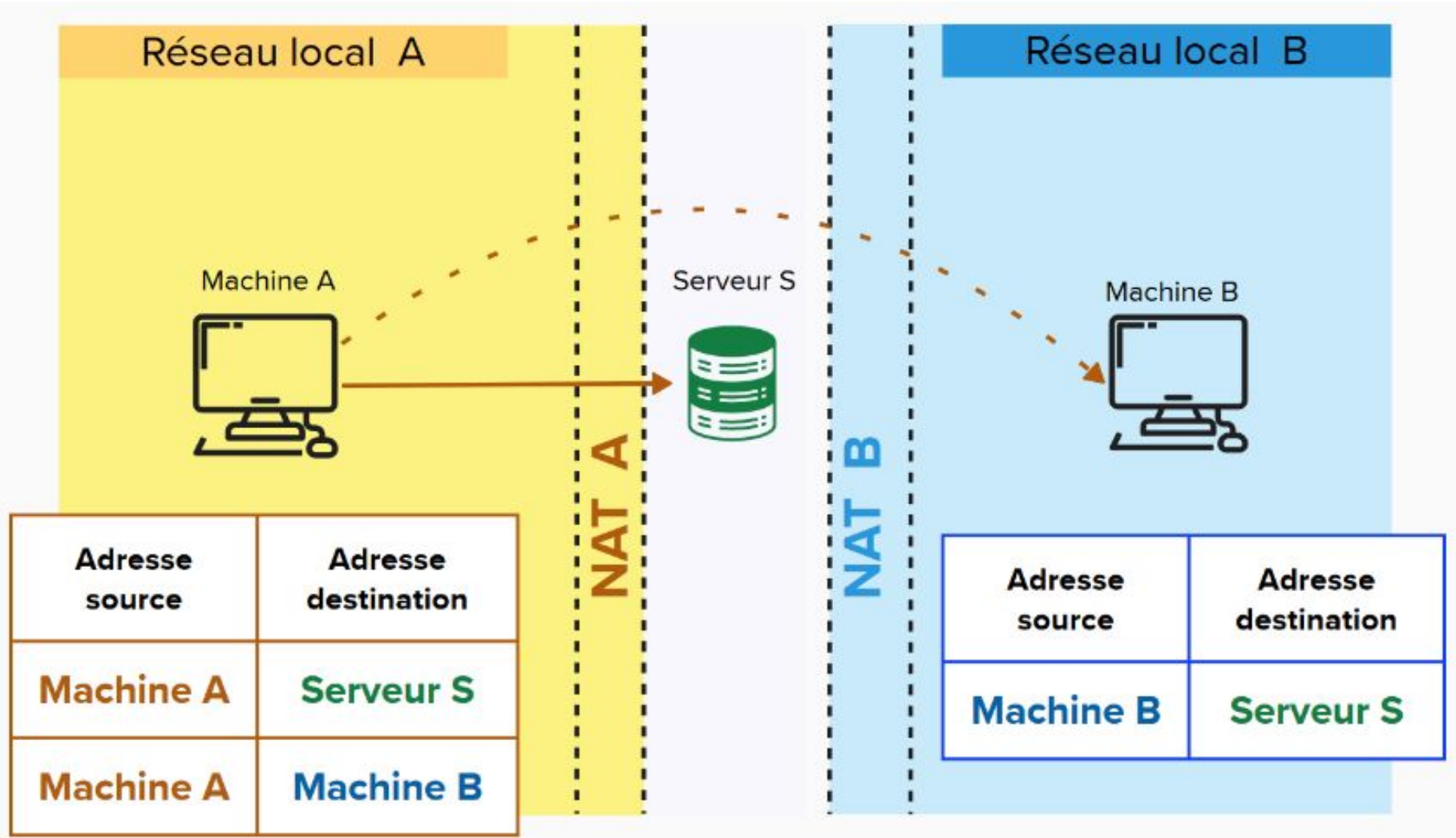
# Connexion Reversal



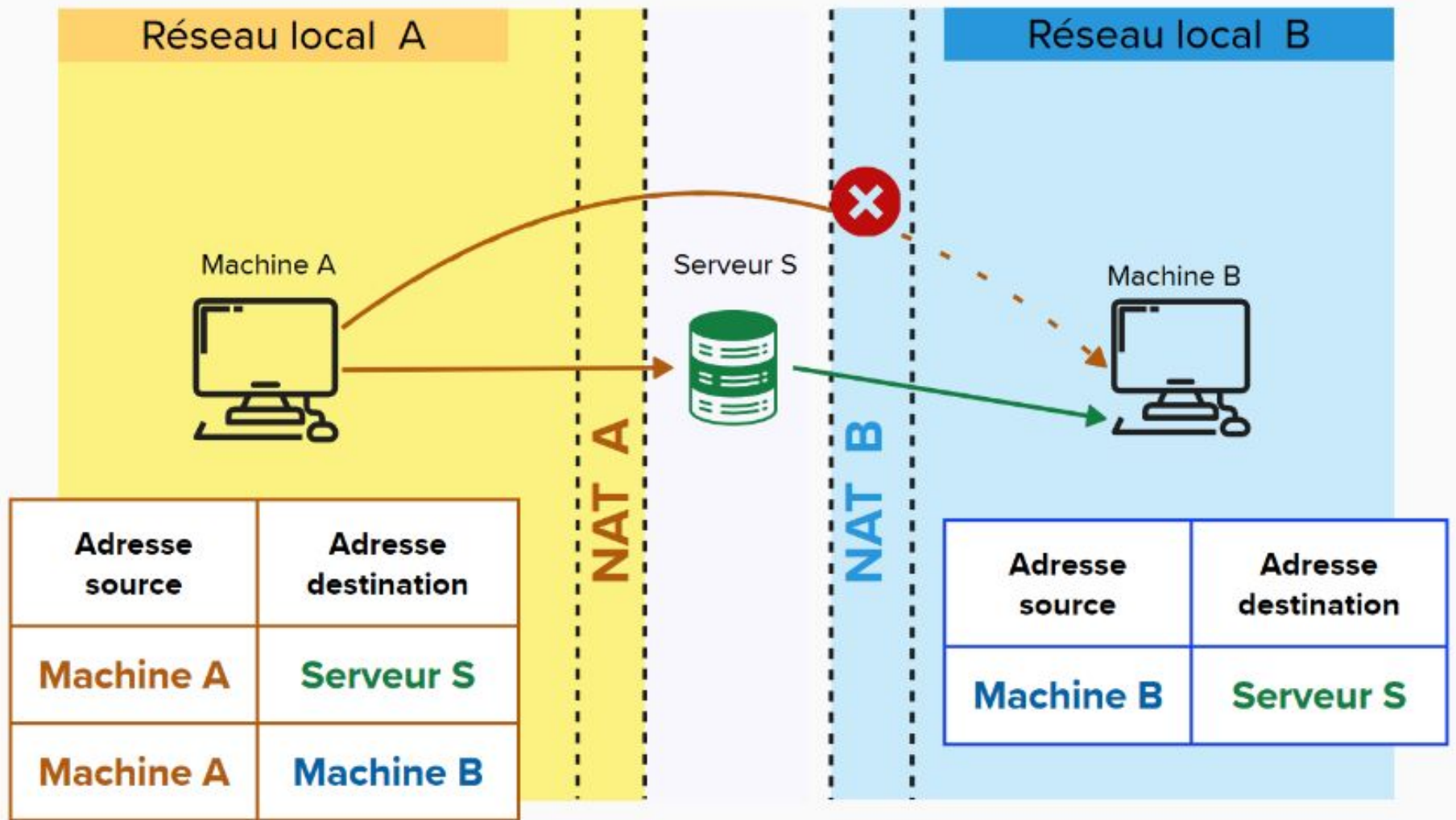
# Connexion Reversal : Avantages et inconvénients

- Avantages :
  - Fonctionne peu importe le type du NAT B
  - Serveur S uniquement sollicité pour la mise en relation
- Inconvénients :
  - Le réseau A ne peut pas être derrière un NAT (sauf Endpoint-Independant Filtering)

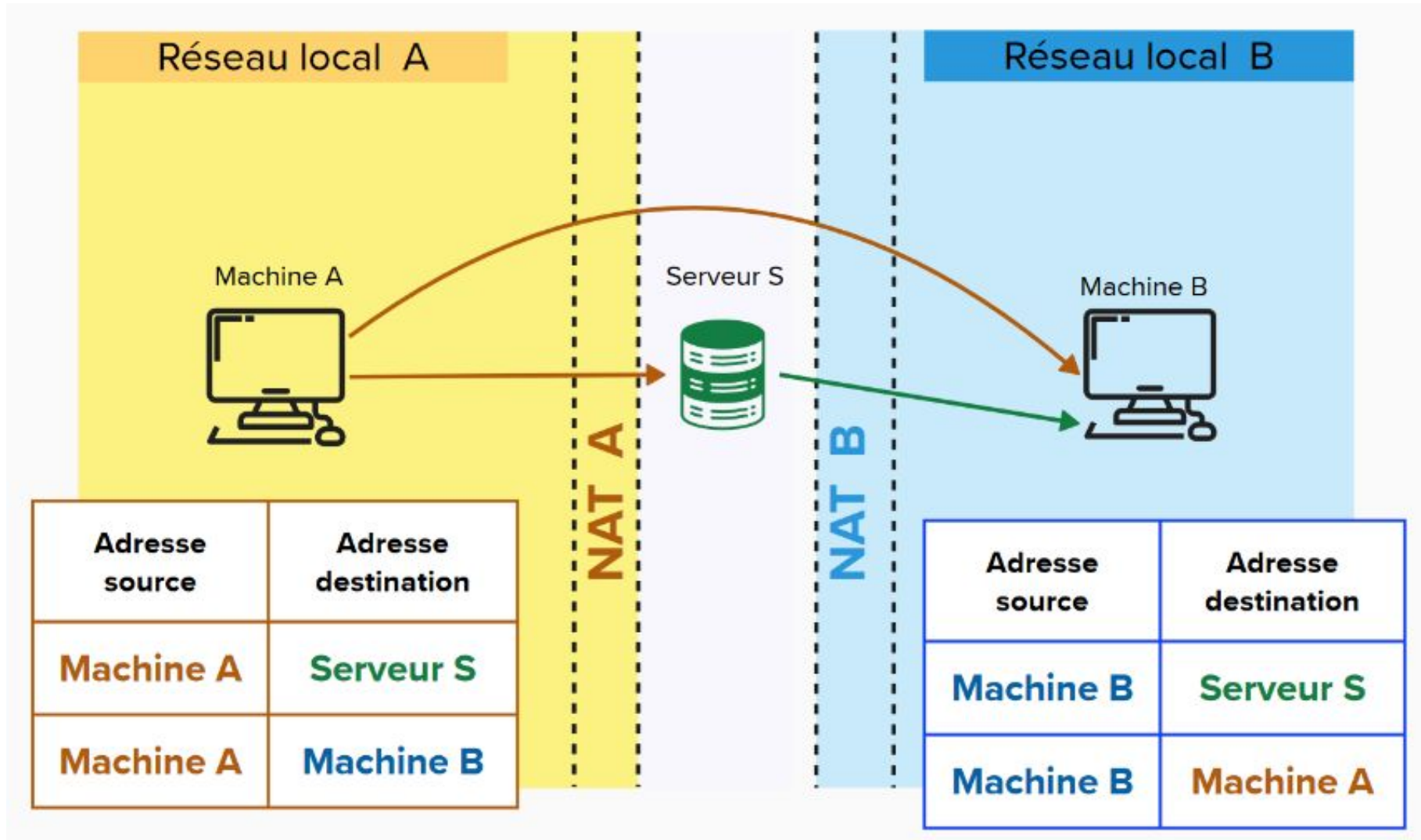
# Hole Punching



# Hole Punching

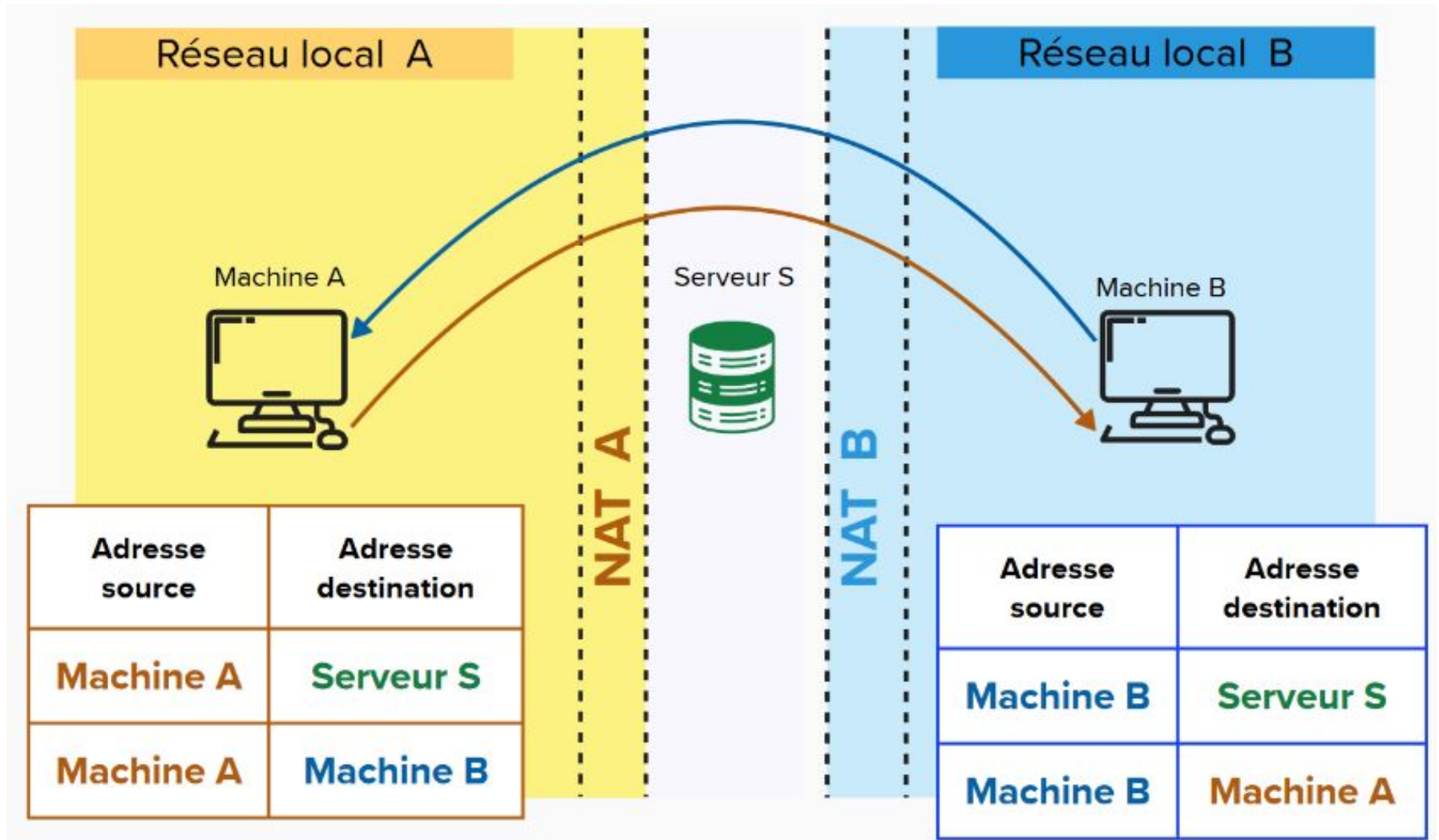


# Hole Punching





# Hole Punching



# Hole Punching : Avantages et inconvénients

- Avantages :
  - Correspond à la plupart des configurations de NAT
  - Serveur S uniquement sollicité pour la mise en relation
- Inconvénients :
  - Nécessite que A et B soient en EIM



# Conclusion & axes de travail

- Pour l'instant, seulement la philosophie de franchissement
- À venir :
  - Implémentation de ces philosophies à travers des protocoles dédiés
  - Apports sécuritaires des NATs

# Bibliographie

C. Jennings, F. Audet. “RFC 4787 - Network Address Translation (NAT) Behavioral Requirements for Unicast UDP”, *Internet Engineering Task Force* (Janvier 2007),

<https://datatracker.ietf.org/doc/html/rfc4787>

P. Srisuresh, B. Ford, D. Kegel. “RFC 5128 - State of Peer-to-Peer (P2P) Communication across Network Address Translators (NATs)”, *Internet Engineering Task Force* (Mars 2008),

<https://datatracker.ietf.org/doc/html/rfc5128>

J. Dordoigne, “Réseaux informatiques - Notions fondamentales” 9ème édition, *ENI Editions* (2022)

S. Guha, K. Biswas, B. Ford, S. Sivakumar, P. Srisuresh. “RFC 5382 - NAT Behavioral Requirements for TCP”, *Internet Engineering Task Force* (Octobre 2008),

<https://datatracker.ietf.org/doc/html/rfc5382>

© Université de Strasbourg