

Maîtriser le Réseau Privé et le NAT sous Proxmox VE

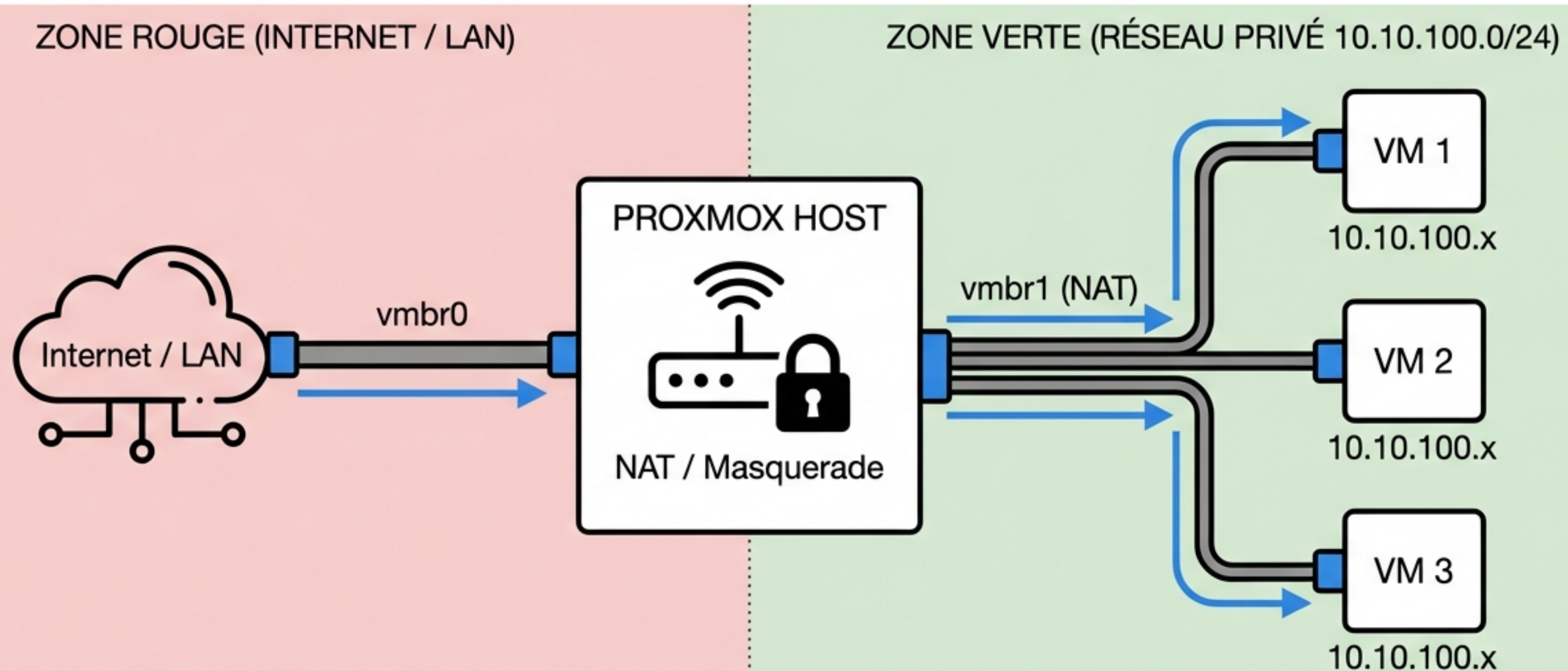
Guide de configuration : du Linux Bridge au Port Forwarding



Basé sur l'expertise technique de IT-Connect

L'Architecture : Créer une zone isolée (Green Zone)

Depuis Proxmox 5.1, l'option de création NAT simple a disparu. Nous devons reconstruire manuellement cette barrière de protection.



Étape 1 : La Fondation (**Configuration GUI**)

Création du Linux Bridge via l'interface Proxmox



Action : Système > Network > Create > Linux Bridge



Insight : Ne pas attacher de ports physiques. Le lien vers l'extérieur se fera logiquement via iptables.

Create: Linux Bridge

Name:

vmbr1

IPv4/CIDR:

10.10.100.1/24

Gateway (IPv4):

Bridge ports:

Comment:

Réseau Interne NAT

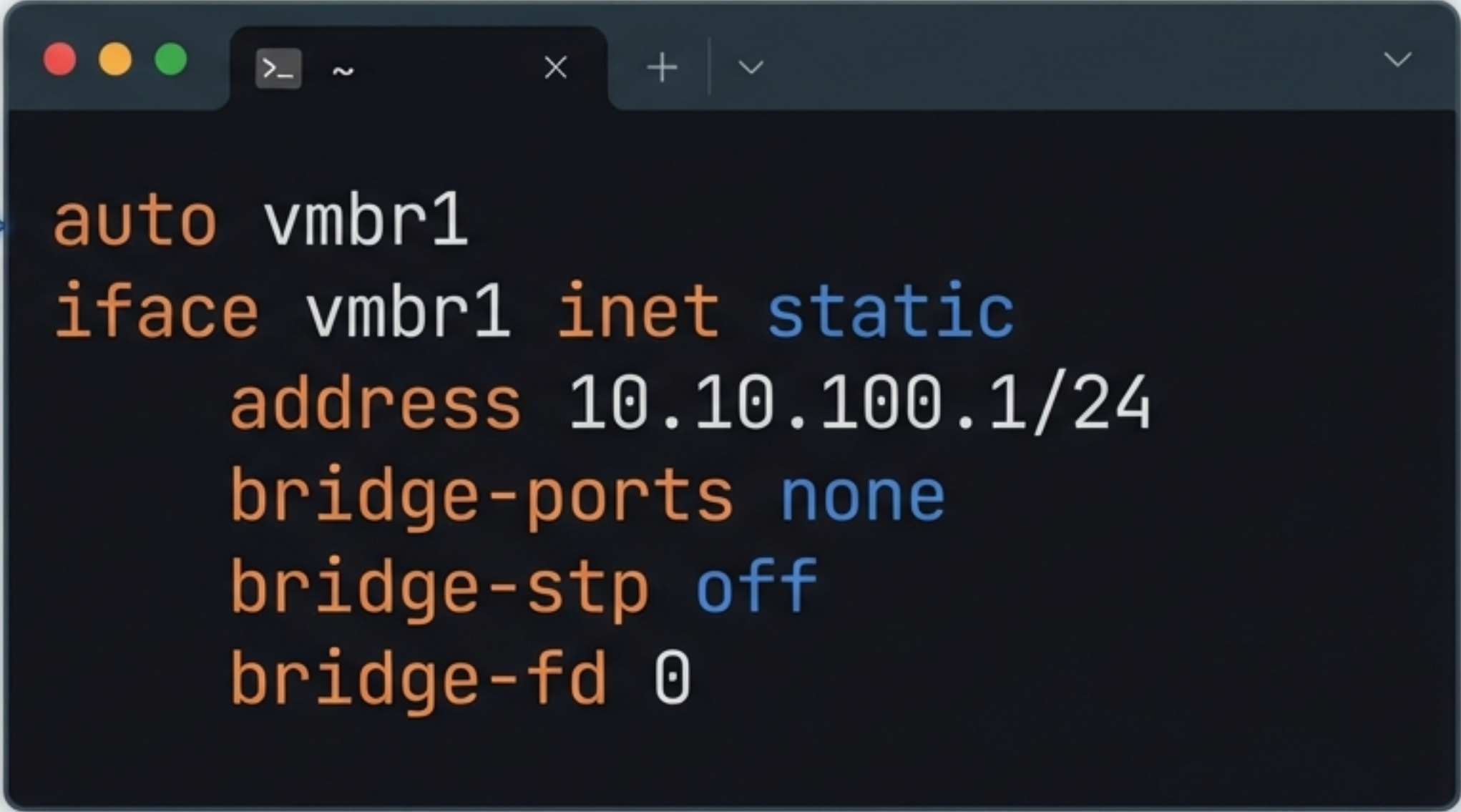
Passerelle pour les VMs

Laisser vide (Isolé)

Étape 2 : Le Câblage Logique (CLI)

Modification du fichier /etc/network/interfaces

+ L'interface créée dans le GUI
apparaît ici. Nous allons
maintenant y injecter
l'intelligence (les règles
post-up).
+



A terminal window with a dark background and a title bar showing a shell prompt. The text is color-coded: 'auto' and 'iface' are orange, 'vmbr1' is white, 'inet' is orange, 'static' is blue, 'address' is orange, '10.10.100.1/24' is white, 'bridge-ports' is orange, 'none' is blue, 'bridge-stp' is orange, 'off' is blue, and 'bridge-fd' is orange. A blue arrow points from the text on the left to the 'vmbr1' in the first line of the terminal output.

```
auto vmbr1
iface vmbr1 inet static
    address 10.10.100.1/24
    bridge-ports none
    bridge-stp off
    bridge-fd 0
```

L'Intelligence du NAT : Masquerade

Activation du routage et de la traduction d'adresse

Active le routage au niveau du noyau Linux (Kernel).

S'applique quand le paquet quitte le serveur.

Interface de sortie (WAN/LAN). Adaptez si nécessaire.

```
post-up    echo 1 > /proc/sys/net/ipv4/ip_forward
post-up    iptables -t nat -A POSTROUTING -s '10.10.100.0/24' -o vmbr0 -j MASQUERADE
post-down  iptables -t nat -D POSTROUTING -s '10.10.100.0/24' -o vmbr0 -j MASQUERADE
```

Action : Sauvegarder et appliquer avec 'systemctl restart networking'

Étape 3 : Le Locataire (Configuration VM)

Attention : Pas de **DHCP**. Le **Linux Bridge** manuel ne fournit pas d'adresses IP. Configuration **statique** requise.

Paramètre	Valeur
Adresse IP (VM)	10.10.100.10
Masque	255.255.255.0 (/24)
Passerelle (Gateway)	10.10.100.1
DNS	1.1.1.1

Internet Protocol Version 4 (TCP/IPv4) Properties

General Alternate Configuration

You can get IP settings assigned automatically if your network reports this capability. If not, you need to ask your network administrator for the appropriate IP settings.

☐ Obtain an IP address automatically

☒ Use the following IP address:

IP address: 10 . 10 . 100 . 10

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 10 . 10 . 100 . 1

☐ Obtain DNS server address automatically

☒ Use the following DNS server addresses:

Preferred DNS server: 1 . 1 . 1 . 1

Alternate DNS server: . . .

☐ Validate settings upon exit

Advanced...

OK Cancel

Vérification de la Connexion Sortante

```
user@vm:~$ ping 1.1.1.1
PING 1.1.1.1 (1.1.1.1) 56(84) bytes of data.
64 bytes from 1.1.1.1: icmp_seq=1 ttl=54 time=14.2 ms
64 bytes from 1.1.1.1: icmp_seq=2 ttl=54 time=13.8 ms
64 bytes from 1.1.1.1: icmp_seq=3 ttl=54 time=14.1 ms
```

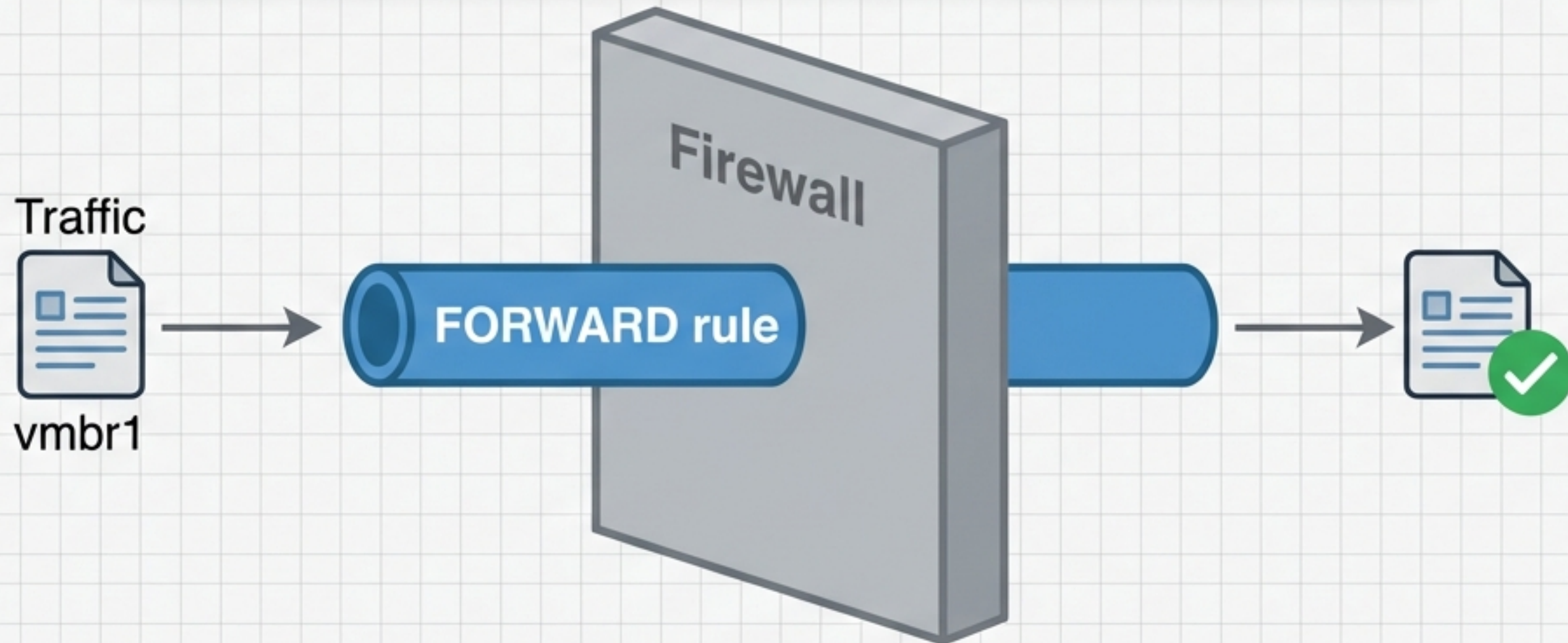


Dépannage : Le 'Mur' du Pare-feu (Méthode CLI)

Autoriser explicitement le transit entre les interfaces

```
/etc/network/interfaces
```

```
post-up iptables -A FORWARD -i vmbr1 -j ACCEPT  
post-up iptables -A FORWARD -o vmbr1 -j ACCEPT
```



Dépannage : Les Bloqueurs Cachés (GUI)

Checklist de sécurité dans l'interface Proxmox

VM 100 (TestVM) - Network Device (net0) ⓧ

Bridge:	vmbr1 ⌵
VLAN Tag:	⌵ ⌶
Firewall:	☒
Model:	VirtIO (paravirtualized) ⌵

Désactivez pour tester.

1. Firewall Option

Hardware > Network Device > Advanced ⓧ

MAC address:		
Rate limit:	0.000	lim/h ⌵
MAC Filter:	☐	
Queues:	2	
Disconnect:	☐	

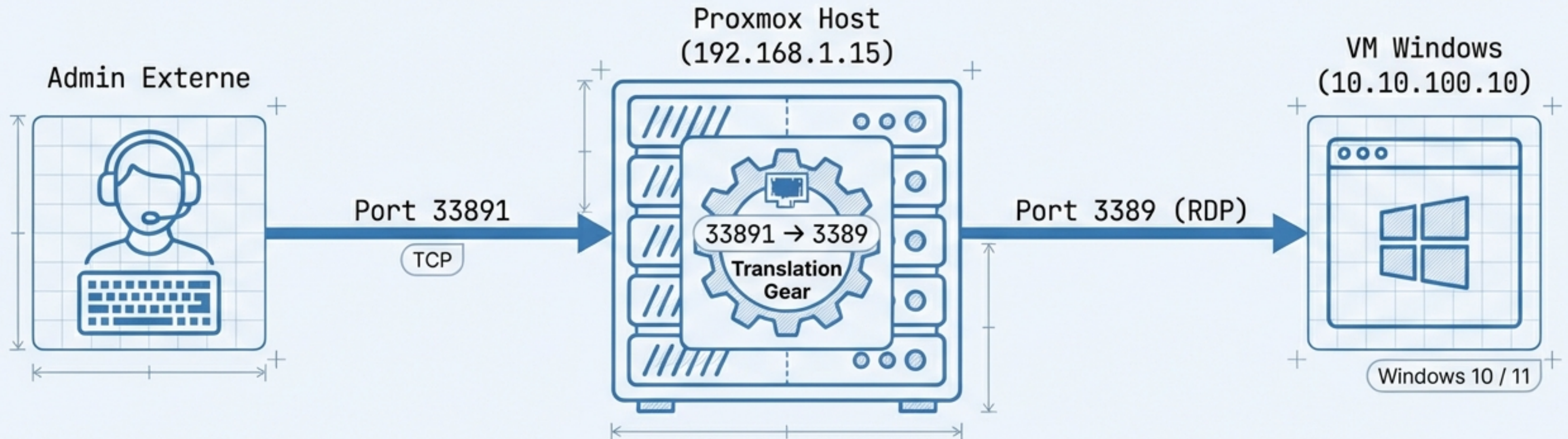
i Peut interférer avec le NAT manuel. Désactivez si nécessaire.

2. MAC Filter

Pro-Tip : Dans le doute, redémarrez le nœud **Proxmox complet** pour vider les tables iptables.

Accès Distant : Le Port Forwarding (DNAT)

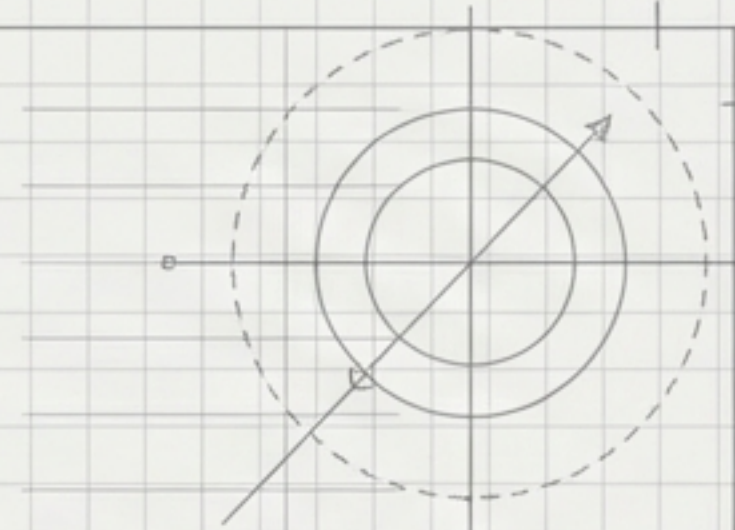
Comment entrer dans le réseau privé ?



Scénario : Accéder au Bureau à distance (RDP) de la VM isolée en passant par un port personnalisé de l'hôte.

Configuration du Port Forwarding

Syntaxe PREROUTING dans **/etc/network/interfaces**

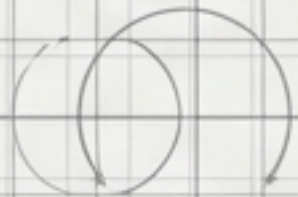


```
# Forwarding RDP (33891 -> 3389)
post-up iptables -t nat -A PREROUTING -i vmbr0 -p tcp --dport
      33891 -j DNAT --to 10.10.100.10:3389
post-down iptables -t nat -D PREROUTING -i vmbr0 -p tcp --dport
      33891 -j DNAT --to 10.10.100.10:3389
```

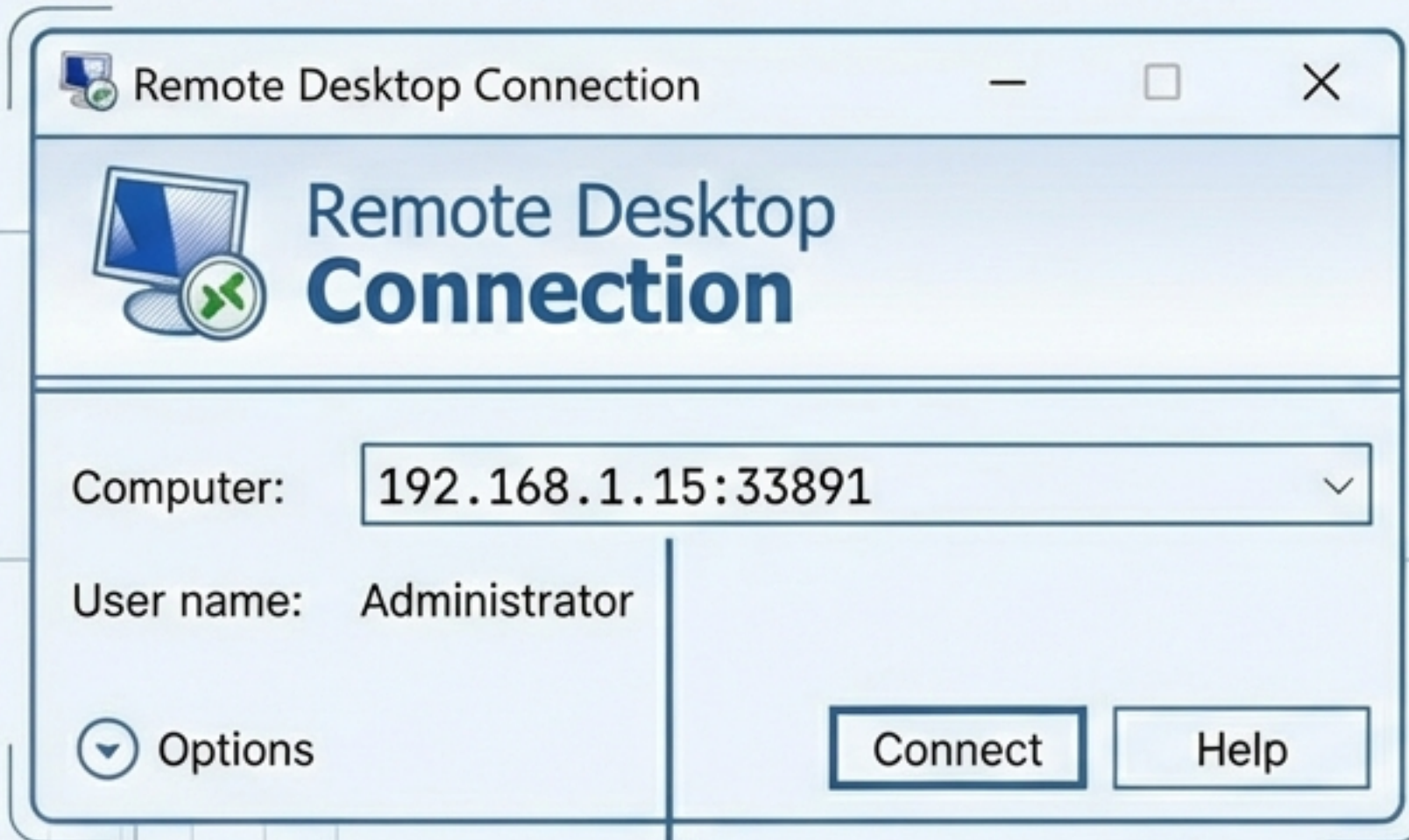
--dport 33891 ← Port exposé sur l'hôte (Entrée)

--to 10.10.100.10:3389 ← Cible interne (IP:Port)

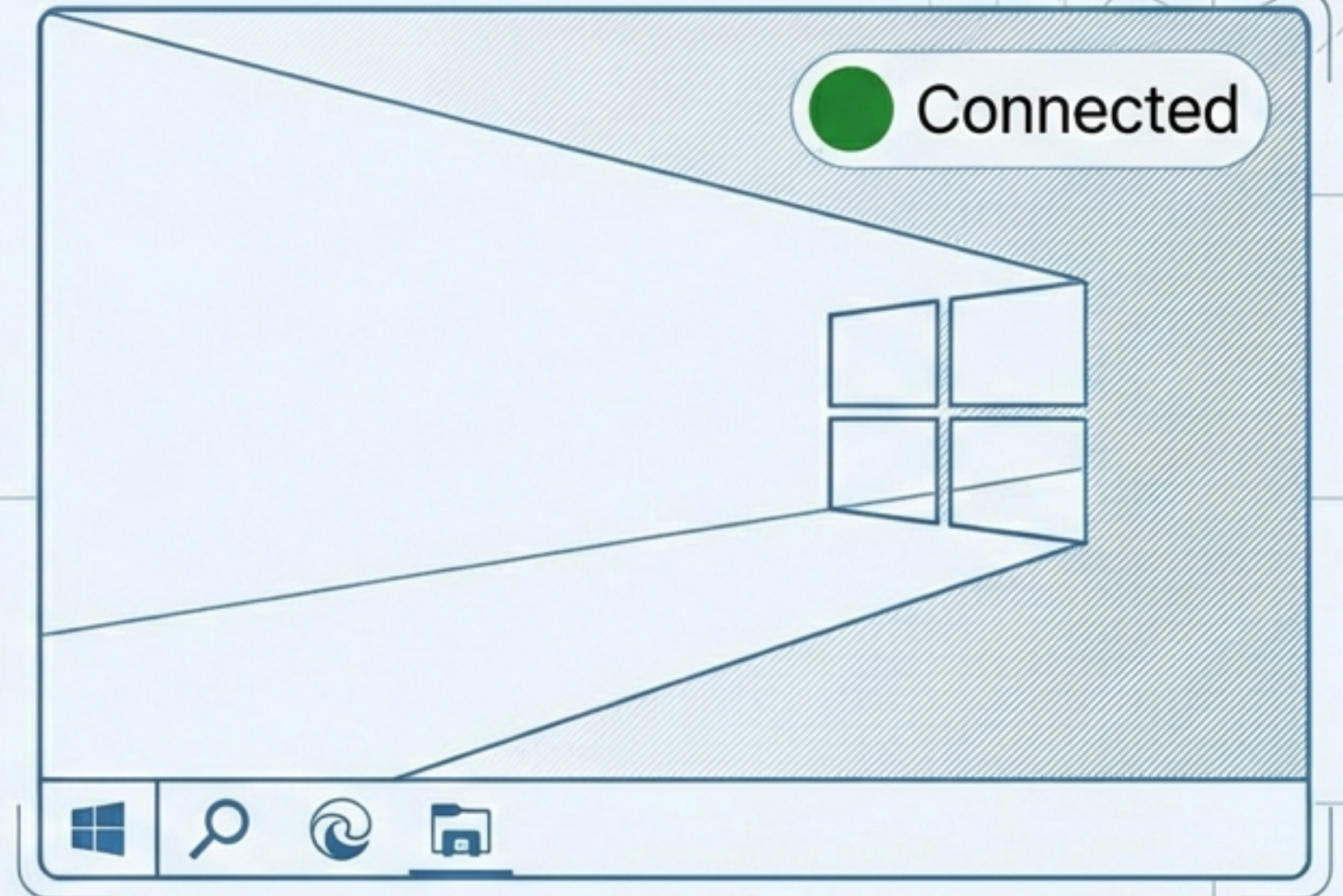
-i vmbr0 ← Interface d'entrée (WAN)



Test de Connexion (RDP)



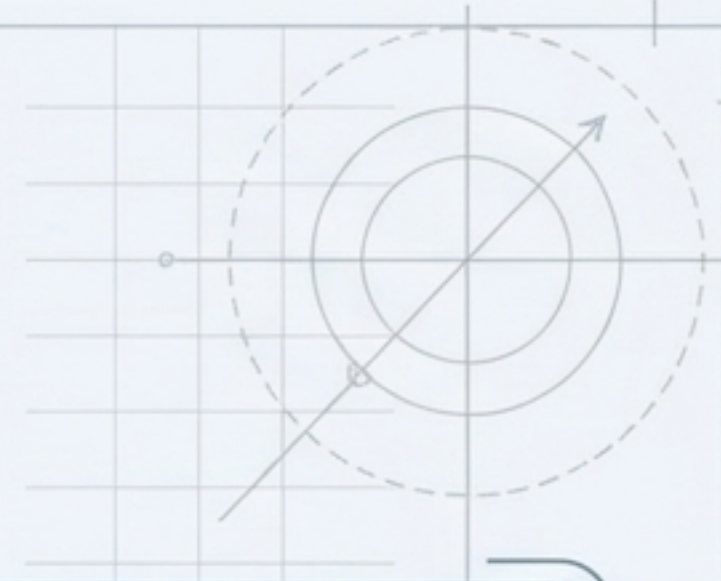
IP du Proxmox + Port Personnalisé



Note : Ne jamais utiliser l'IP 10.10.x.x depuis l'extérieur. Elle est invisible.

L'Aide-Mémoire (Cheat Sheet)

Toutes les commandes essentielles sur une page



1. Activer le Routage

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

2. Outbound NAT (Masquerade)

```
iptables -t nat -A POSTROUTING -s '10.10.100.0/24' -o vmbr0 -j MASQUERADE
```

3. Inbound NAT (Port Forwarding)

```
iptables -t nat -A PREROUTING -i vmbr0 -p tcp --dport [PORT_EXT] -j DNAT  
--to [IP_VM]:[PORT_INT]
```

Rappel : Pour chaque règle 'post-up -A', ajoutez une règle 'post-down -D' correspondante pour le nettoyage.

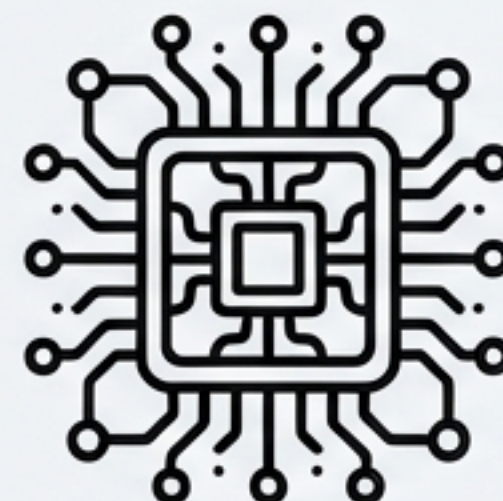
Aller plus loin : L'alternative SDN

Linux Bridge
(Méthode Manuelle)



La méthode Linux Bridge est robuste et universelle. Cependant, pour des déploiements complexes, Proxmox offre désormais le SDN.

Proxmox SDN
(Software Defined Network)



Le SDN inclut une fonction SNAT (Source NAT) native qui automatise ce processus via l'interface graphique.