# Les Modes d'Accès Réseau

# 1. 🌐 NAT (Network Address Translation)

- **Principe** : La machine virtuelle (VM) utilise l'adresse IP de l'hôte pour sortir sur Internet.
- Elle est cachée derrière l'hôte.
- **Avantage** : Internet accessible, pas d'exposition directe de la VM.
- **Inconvénient** : La VM ne peut pas être jointe directement depuis l'extérieur.
- **Utilisation typique** : Navigation web, mises à jour, tests simples.

## Comment fonctionne le mode NAT ?

- La VM a sa propre adresse IP privée **(ex: 10.0.2.15)**.
- Elle passe par une sorte de routeur virtuel intégré à l'hyperviseur (comme VirtualBox, VMware…).
- Ce routeur utilise l'IP publique de ton hôte pour sortir vers Internet (comme une box internet).
- Donc ta VM accède à Internet via l'hôte, mais l'hôte ne peut pas être accédé depuis la VM directement (sauf si on ouvre manuellement des ports).

## Est-ce qu'un virus sur la VM peut toucher l'hôte ?

La réponse est non sauf si

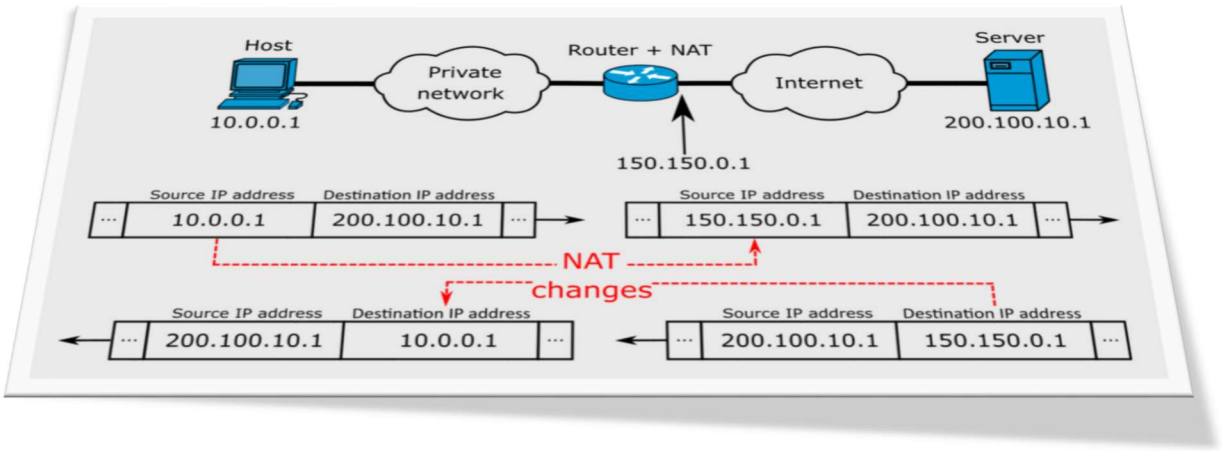
- On partage des dossiers entre la VM et l'hôte (fonction "shared folders").
- Copié/collé activé entre les deux.
- Glisser-déposer activé.
- Mauvaise configuration de l'hyperviseur (mode "bridged", par exemple, ou pas de sandbox).

Sinon, en mode NAT bien isolé :

- Le virus reste dans la VM, comme dans une boîte de test.
- Il n'a pas accès au système de l'hôte, ni à ses fichiers.

Même en NAT, voici les dangers si :

- On navigue dans la même session sur ton hôte et VM et ouvres les mêmes comptes (phishing, token volé…).
- Le virus se propage via le réseau local si l'hôte et la VM partagent un LAN visible.
- Téléchargement d'un keylogger ou ransomware dans un dossier partagé sans faire attention.




# 2. 🕌 Accès par pont (Bridged Network)

- **Principe** : La VM est directement connectée au réseau physique de l'hôte, comme une machine réelle.
- Elle a sa propre IP (fournie par le DHCP du réseau local).
- **Avantage** : Elle peut communiquer avec toutes les autres machines du réseau, comme un vrai PC.
- **Inconvénient** : Moins sécurisé, plus exposé au risques décrit dans le NAT.
- **Utilisation** : Simulations réseau, accès direct, test de serveurs.

## Comment fonctionne le mode par pont ?

• La VM reçoit une adresse IP du même réseau local que ton PC hôte.

• Elle partage directement la carte réseau physique de ton hôte, comme s'il s'agissait d'une deuxième machine branchée à la box/routeur.

• Elle peut communiquer avec d'autres appareils du réseau (imprimantes, autres PC, NAS, Internet…) sans passer par l'hôte**.**

⚠️ Mais attention la VM est exposée au réseau local, donc aux virus, attaques, etc. et contrairement au mode NAT, il n'y a **aucune barrière** entre hôte et VM.

## Quand utiliser le mode "Accès par pont" ?

- Pour **tester un serveur web localement** accessible depuis d'autres appareils.
- Pour **faire du pentest sur un vrai réseau local**.
- Pour **avoir une adresse IP différente** que celle de l'hôte.

# 3. 🏠 Réseau interne (Internal Network)

- **Principe** : Les VMs peuvent communiquer entre elles, mais pas avec l'hôte ni avec Internet.
- **Avantage** : Très isolé, idéal pour tester des protocoles ou services réseau entre VMs, Pentest.
- **Inconvénient** : Pas d'accès Internet (peut être résolu si 2 interfaces réseau NAT et Interne).
- **Utilisation** : Tests d'attaques internes, LABs cybersécurité.

## Comment fonctionne le mode interne ?

- La VM ne peut parler qu'aux autres VMs configurées sur le même réseau interne**.**
- Aucun accès à l'hôte.
- Aucun accès à Internet.
- Idéal pour simuler un réseau fermé**,** sans aucune sortie vers l'extérieur**.**

# 4. Réseau privé de l'hôte (Host-Only Network)

- **Principe** : La VM peut communiquer avec l'hôte, mais pas avec Internet**.**
- **Avantage** : Bon pour échanger entre hôte et VM (FTP, scripts, etc.).
- **Inconvénient** : Toujours isolé du réseau global.
- **Utilisation** : Test de services locaux, lab d'administration système.
-

## Comment fonctionne le mode Host-Only Network ?

- La VM et l'hôte sont dans un réseau privé virtuel créé par l'hyperviseur.
- Ils ont tous les deux une adresse IP dans un sous-réseau privé (souvent en 192.168.x.x).
- La VM ne peut pas accéder à Internet, sauf si un mécanisme de routage est mis en place manuellement.

## Quand utiliser le réseau privé de l'hôte ?

- Pour tester une application client/serveur entre hôte et VM**.**
- Pour partager des fichiers ou services localement sans exposition au réseau.
- Pour s'entraîner sur la configuration de réseau privé.

## 5. Generic Driver

- **Principe** : Permet d'utiliser un pilote réseau personnalisé (peu utilisé en pratique).
- Réservé à des cas très techniques.
- **Exemple** : Emuler un comportement réseau spécifique avec un driver maison.

**À éviter si tu ne sais pas exactement pourquoi tu en as besoin.**

---

## 6. ☁️ Cloud Network *(spécifique à certaines solutions comme Oracle VirtualBox, VMware Cloud, etc.)*

- **Principe** : La VM est connectée à un réseau cloud privé (fournisseur externe).
- Géré souvent par des API ou portails de cloud.
- **Avantage** : Très scalable et accessible à distance.
- **Inconvénient** : Configuration plus complexe, dépendance au fournisseur.
- **Utilisation** : Cloud labs, déploiement pro, architecture cloud.