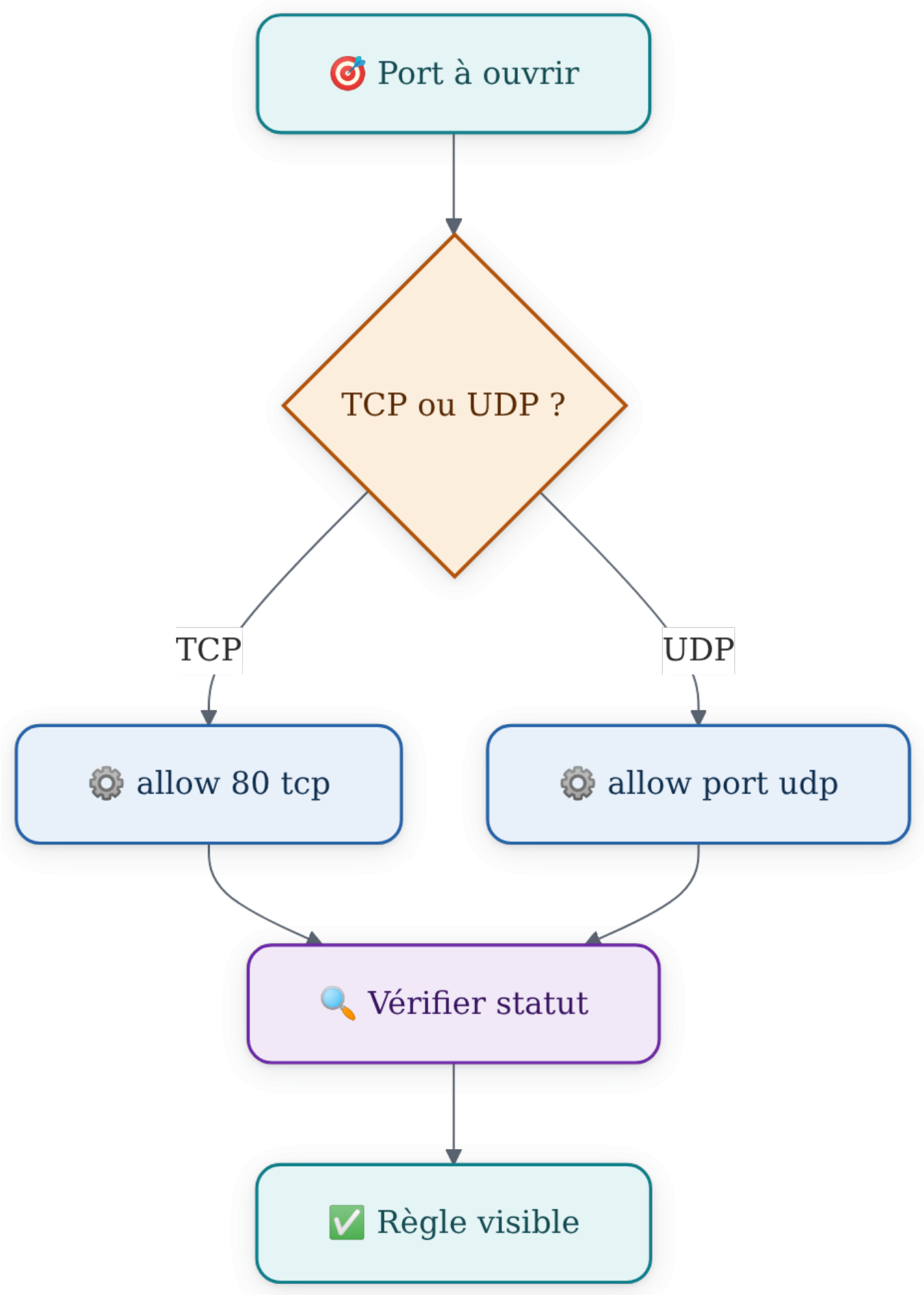
UFW sous Ubuntu : ouvrir, vérifier et retirer une règle sans perdre l'accès

Suivez ce parcours avant toute modification du pare-feu, particulièrement sur un serveur accessible à distance. Chaque étape vise à limiter l'exposition réseau tout en conservant un accès d'administration fonctionnel.

Au sommaire

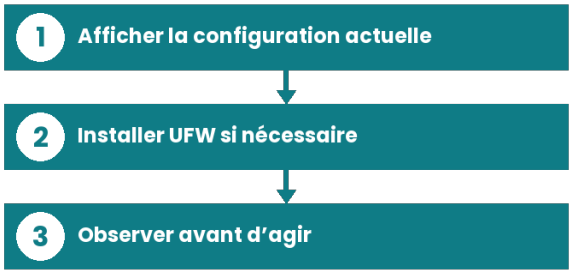
Avant de modifier une règle

- [ ] **Identifier le service concerné**
  Une règle UFW filtre l'accès réseau ; elle ne démarre pas le service.
- [ ] **Vérifier le port et le protocole attendus**
  Choisissez TCP, UDP ou les deux selon la documentation du logiciel.
- [ ] **Prévoir un test depuis une autre machine**
  Conservez votre session SSH actuelle ouverte pendant le test.
- [ ] **Éviter les ouvertures générales inutiles**
  N'ouvrez qu'un port, une plage ou une source IP réellement nécessaire.


🎯 Port à ouvrir
TCP ou UDP ?
TCP
UDP
⚙️ allow 80 tcp
⚙️ allow port udp
🔍 Vérifier statut
✅ Règle visible

INFOGRAPHIE *Schéma pour ouvrir un port Ubuntu avec UFW et vérifier une règle TCP ou UDP*

1. Contrôler l'état d'UFW



1 **Afficher la configuration actuelle**
Exécutez : sudo ufw status. La commande indique si UFW est actif et affiche les règles appliquées.

2 **Installer UFW si nécessaire**
Si la commande n'existe pas, installez le paquet avec : sudo apt install ufw

3 **Observer avant d'agir**
Ne modifiez ou ne supprimez pas une règle sans avoir identifié son rôle dans la liste affichée.

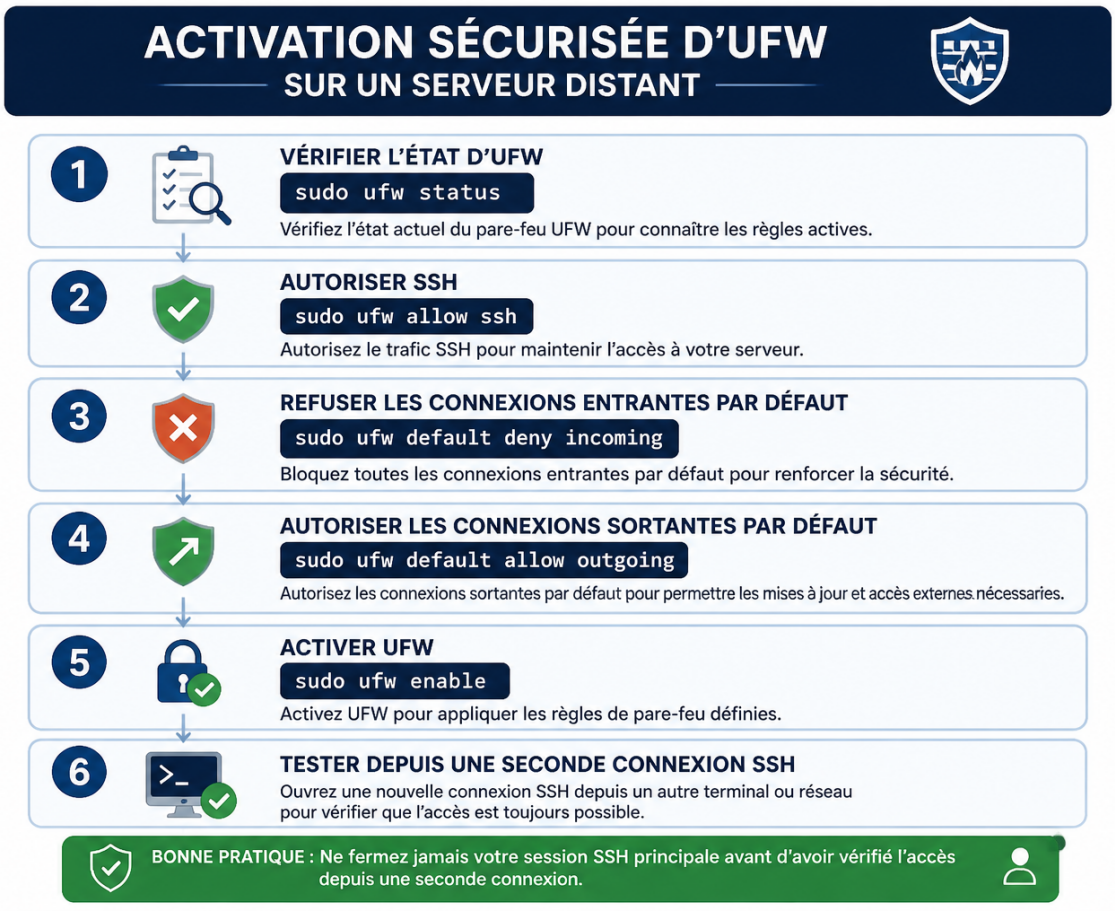
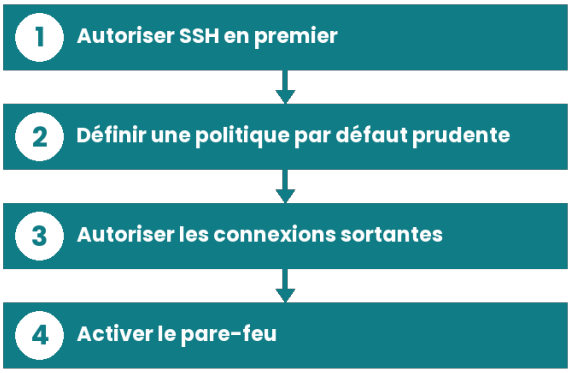


SCHÉMA *Séquence de sécurité à suivre avant d'activer UFW sur un serveur administré en SSH.*

2. Activer UFW sans couper SSH



1 **Autoriser SSH en premier**
Sur une machine distante, exécutez : sudo ufw allow ssh

2 **Définir une politique par défaut prudente**
Refusez les connexions entrantes non prévues avec : sudo ufw default deny incoming

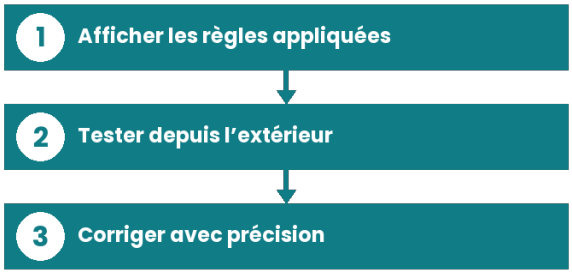
3 **Autoriser les connexions sortantes**
Exécutez : sudo ufw default allow outgoing

4 **Activer le pare-feu**
Exécutez : sudo ufw enable, puis testez une nouvelle connexion SSH depuis une seconde machine avant de fermer la session en cours.

3. Choisir la bonne commande d'ouverture

Besoin	Commande UFW	Point de contrôle
Autoriser HTTP en TCP	sudo ufw allow 80/tcp	Un service HTTP doit réellement écouter sur la machine.
Autoriser un port UDP	sudo ufw allow 53/udp	Utilisez UDP uniquement si le service le demande.
Autoriser SSH par son nom	sudo ufw allow ssh	À appliquer avant l'activation d'UFW sur un serveur distant.
Autoriser une plage TCP requise	sudo ufw allow 30120:30130/tcp	À réserver aux logiciels qui exigent explicitement une plage.
Restreindre l'accès à une adresse IP	sudo ufw allow from 192.0.2.10	Remplacez cette adresse d'exemple par l'IP stable de la machine autorisée.

4. Vérifier l'ouverture avant de considérer le travail terminé

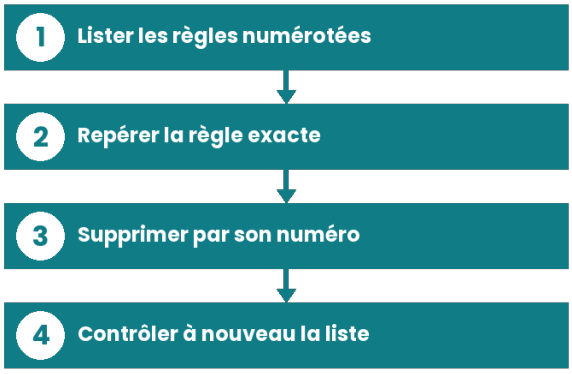


1 **Afficher les règles appliquées**
Exécutez : sudo ufw status. Vérifiez que la règle, le port et le protocole correspondent à votre besoin.

2 **Tester depuis l'extérieur**
Testez l'accès depuis une autre machine lorsque cela est possible. Une règle visible dans UFW ne garantit pas qu'un service fonctionne ou écoute.

3 **Corriger avec précision**
Si le protocole choisi ne correspond pas au service, retirez la règle erronée puis créez la règle adaptée.

5. Fermer un port ou supprimer une règle



1 **Lister les règles numérotées**
Exécutez : sudo ufw status numbered

2 **Repérer la règle exacte**
Vérifiez le port, le protocole et le sens de la règle avant toute suppression.

3 **Supprimer par son numéro**
Exécutez : sudo ufw delete <numéro>

4 **Contrôler à nouveau la liste**
Relancez : sudo ufw status numbered. Les numéros des règles changent après une suppression.

! **Point de vigilance : accès distant**
N'activez pas UFW sur un serveur distant avant d'avoir autorisé SSH. Gardez la connexion actuelle ouverte et validez l'accès avec une seconde connexion avant toute déconnexion.

Adaptez toujours le port et le protocole à la documentation du service exposé.