**TP Administration : Pare-Feu**

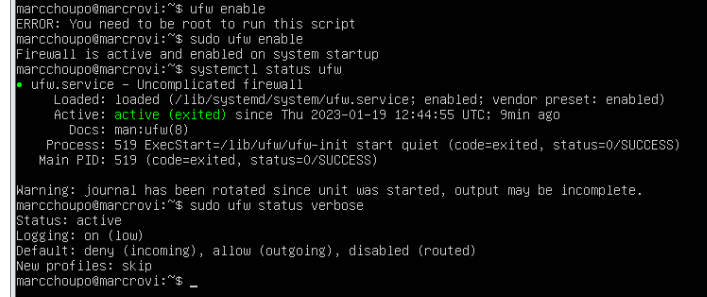
**Réponses Aux Questions**

1. \* Vérifions m’état de UFW

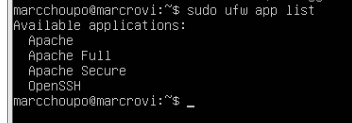


1. Activons UFW et

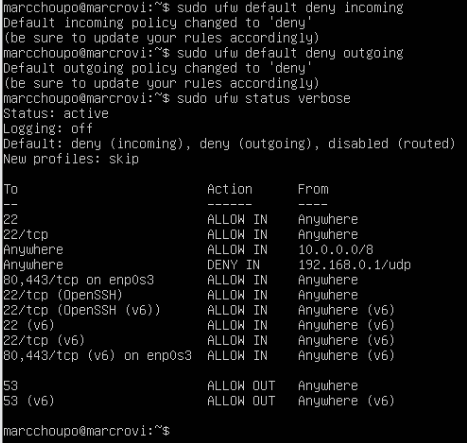
3) Vérifions son état

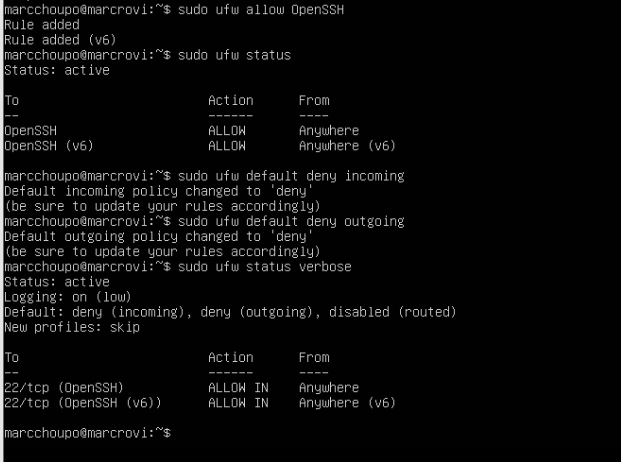


* La politique de filtrage par défaut stipule que Par défaut, cette politique de filtrage est activée en configuration d’usine.  
  Seuls les ports correspondant à l'administration du firewall sont ouverts (1300/TCP et 443/TCP). Le test d’accessibilité PING à destination de toutes les interfaces du firewall est également autorisé. Toutes les autres connexions sont ensuite bloquées.

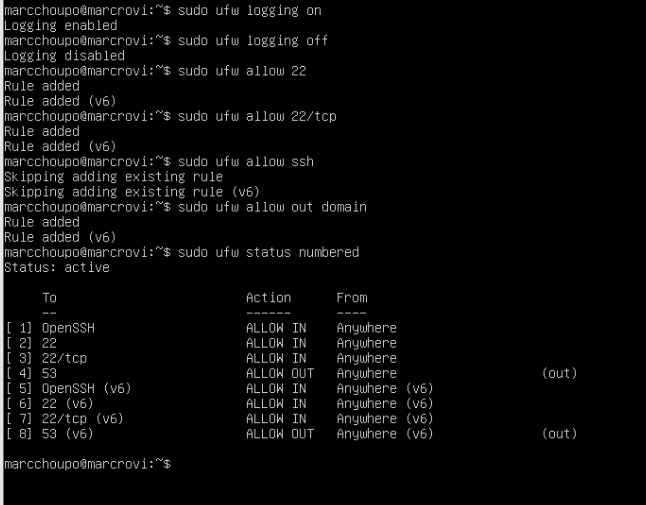


1. Autorisons les connexions SSH puis vérifions l’état de UFW, politiques incoming et outgoing

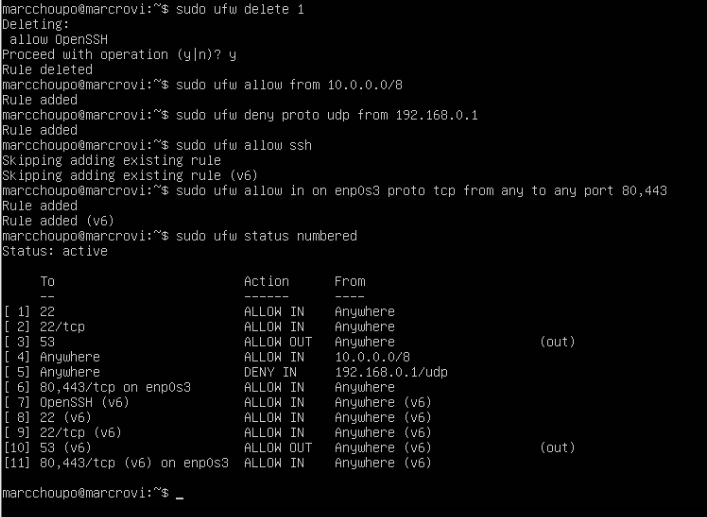


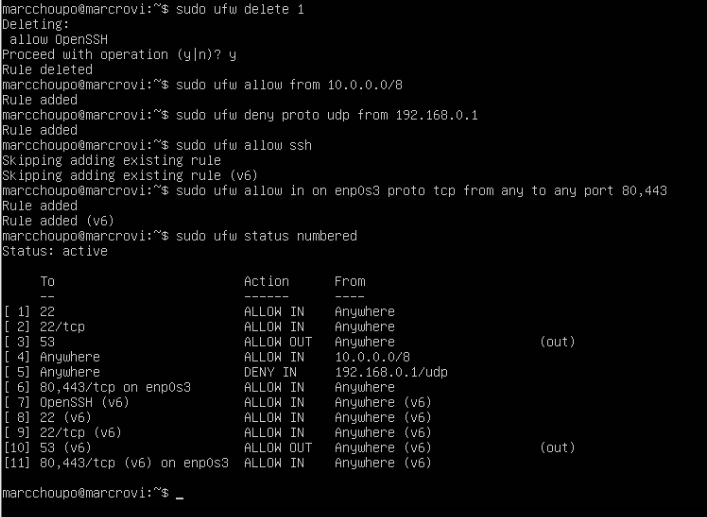


* **Journalisation**

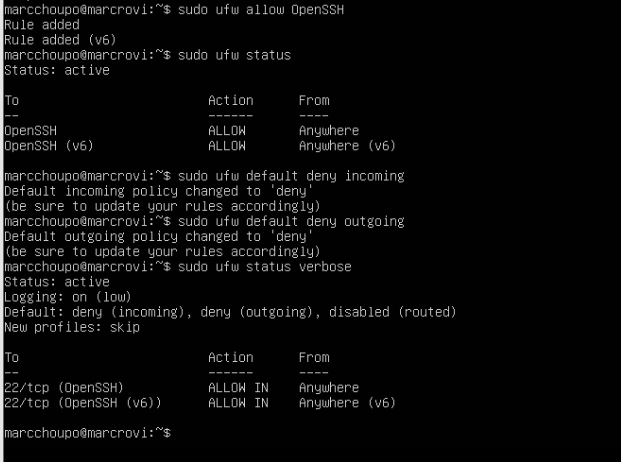


* Visualisation des règles et de leurs numéros

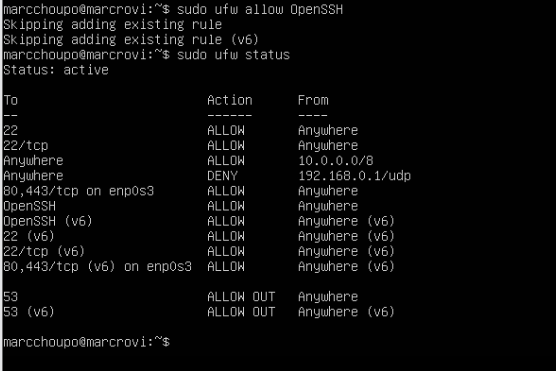




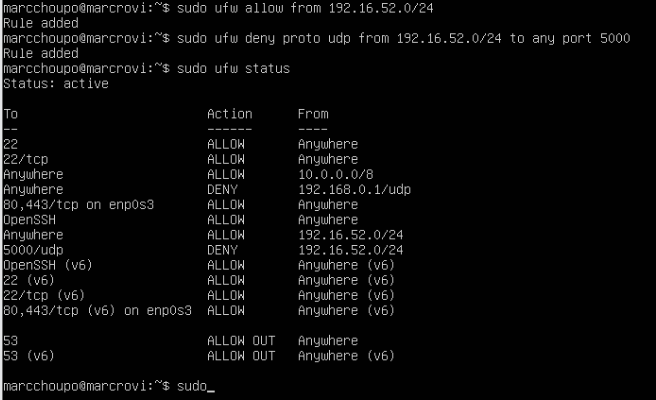
1. Mettons en place une politique de close config par défaut



1. Autorisons le service SSH

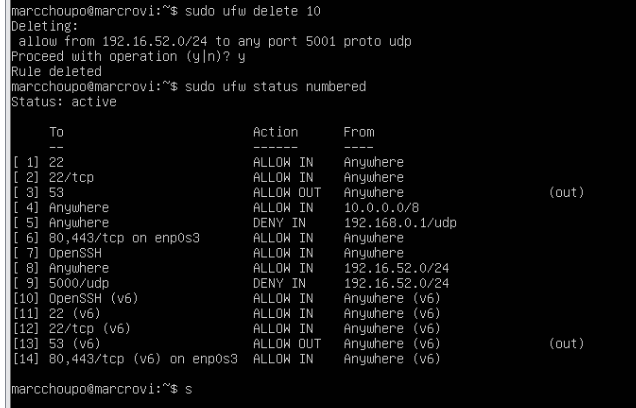


1. Autoriser et interdire le trafic local du réseau 192.168.52.0/24.









1. Interdisons la possibilité de pinger le serveur

