

## Atelier du samedi 3 décembre 2022 - 9 heures 30 - 17 heures 30 - iptables/nftables

**NetFilter/iptables** est un **pare-feu (Firewall) Linux** qui est un dispositif logiciel permettant de filtrer les paquets réseau afin de mettre en place une politique de sécurité.

**Nftables** est un sous-système du noyau Linux fournissant le filtrage et la classification des paquets, disponible depuis le noyau Linux 3.13. **Nftables**, ayant pour ambition de remplacer **iptables**, est aussi censé remplacer certaines parties de **Netfilter**, tout en les conservant et les réutilisant.

Parmi les avantages de **nftables** sur **netfilter**, il y a **moins de duplication de code et plus de débit**. **Nftables** est configuré via **l'utilitaire espace utilisateur nft**, tandis que **netfilter** est configuré via les **utilitaires iptables, ip6tables, arptables et ebtables**. **Nftables** utilise les blocs de construction de l'infrastructure **Netfilter**, tels que les points d'ancrage existants dans la pile de réseau, le système de suivi de connexion, le composant de mise en file d'attente de l'espace utilisateur et le sous-système de journalisation.

Cet atelier sera l'objet de présenter **Iptables/Nftables** et les nouveautés apportées par **Nftables**. Cet atelier permettra de passer en revue les **tables (Filter, NAT, Mangle)**, les **chaines (INPUT, POSTROUTING, etc.)**, le **suivi de connexion** ainsi que les **cibles (ACCEPT, DROP, etc.)**. Une comparaison entre **Iptables/Nftables** sera faite.

Certains concepts réseaux seront abordés et mis en pratique avec un **environnement Docker et GNS3**. Pour ceux qui n'ont pas suivi l'atelier sur la mise en place de l'environnement Docker et GNS3, vous pouvez vous référer à la procédure d'installation ci-jointe. En cas de non installation de l'environnement, une **VM Debian** avec l'ensemble des outils installés fonctionnant sous **VirtualBox** et **VMWare Workstation** vous sera fournie le jour de l'atelier.