Blocage d'Internet pour les sessions élèves

Il peut arriver qu'on ne veuille pas que les élèves en maternelle (utilisateur "Jerry") aient accès à Internet tout en gardant cette possibilité pour le compte Poe de l'enseignant·e et les autres élèves (utilisateurs "Koda et "Leon").
La solution repose sur nftables qui est assez peu utilisé face à son prédécesseur iptables.

Voir cette page pour plus d'info sur nftables : https://fr.wikipedia.org/wiki/Nftables

EN COURS DE TEST : RETOURS APPRÉCIÉS !!!

On va d'abord trouver l'UID de l'utilisateur Jerry avec la commande :

```
id -u jerry
```

Ça nous retourne un nombre. Pour Jerry, l'UID est :

```
1001
```

On peut dès lors éditer le fichier de configuration de nftables avec la commande :

```
sudo nano /etc/nftables.conf
```

Voici le contenu initial :

```
#! /usr/sbin/nft -f

flush ruleset

table inet filter {
        chain input {
                type filter hook input priority filter;
        }
        chain forward {
                type filter hook forward priority filter;
        }
        chain output {
```

```
                type filter hook output priority filter;
        }
}
```

On va alors ajouter dans la partie "chain output", les règles pour l'utilisateur ayant l'UID 1001 qui est Jerry :

```
#! /usr/sbin/nft -f

# Paramètres à adapter selon l'UID de Jerry et votre réseau LAN
# Il suffit d'initialiser les variables nécessaires uniquement dans cette partie
define UTILISATEUR = 1001
# Pour plusieurs utilisateurs UID 1001 (Jerry), 1002 (Koda) et 1003 (Léon)
# et remplacer $UTILISATEUR par $UTILISATEURS défini ci-dessous
#define UTILISATEURS = { 1001, 1002, 1003 }
define LAN = 192.168.1.0/24

# Suppression des règles existantes (remise à zéro)
flush ruleset

# Règles à appliquer
table inet filter {
    chain input {
        type filter hook input priority filter;
    }

    chain forward {
        type filter hook forward priority filter;
    }

    chain output {
        type filter hook output priority 0;
        # les règles "accept" doivent précéder les règles "drop" !!!
        # Loopback / localhost
        meta skuid $UTILISATEUR oif lo accept
        # LAN IPv4
        meta skuid $UTILISATEUR ip daddr $LAN accept
        # LAN IPv6
        meta skuid $UTILISATEUR ip6 daddr { fe80::/10, fc00::/7 } accept
        # Blocage total Internet avec message indiquant que la connexion est refusée
```

```
        meta skuid $UTILISATEUR reject with icmpx type admin-prohibited
        # ou Blocage total sans message avec Timeout
        #meta skuid $UTILISATEUR drop

    }
}
```

On applique la config avec cette commande :

```
sudo nft -f /etc/nftables.conf
```

Pour rendre cette règle pérenne au démarrage, taper les commandes :

```
sudo systemctl enable nftables
sudo systemctl restart nftables
```

Pour vérifier les règles, taper :

```
sudo nft list ruleset
```

Revision #9
Created 19 March 2026 07:27:03 by Thierry
Updated 26 March 2026 13:26:37 by Thierry