nftables memo

Memo sur la gestion du pare-feu netfilter, via l'outil nftables.
Les commandes essentielles sont présentées, avec des exemples.

Gestion des tables

Création d'une table:

```
nft add table add inet example_filter
```

Ici notre table se nomme "example_filter".

- inet: table ipv' et ipv-
- ip: table ipv4
- ip6: table ipv6
- arp: table pour arp

Pour la liste des tables: Wiki nftable

Suppression d'une table :

```
nft delete table inet example_filter
```

Lister le contenu d'une table:

```
nft list inet example_filter
```

Gestion des chaines

Ensuite il va falloir ajouter des chaines à notre table et les lier à des "*hooks*". Ces derniers vont définir à quel type de hook de netfilter ils sont rattachés.

Ces chaines peuvent avoir n'importe quel nom, du moment qu'elles sont rattachées au bon hook (input, output...).

Ici on va créer une chaine "INPUT" et "OUPUT" pour que ça soit clair, mais on aurait pu les appeler autrement, du moment qu'ils bien rattachés aux hook:

```
nft add chain inet filter input '{type filter hook input priority 0;}'


nft add chain inet filter output '{type filter hook output priority 0;}'
```

Ici le "priority 0" faut référence à la priorité de la table, c'est à dire l'ordre de prise en compte des chaines. Par défaut c'est 0, mais on aurait pu créer plusieurs type de chaines, liées au hook 'input', mais avec des priorité déférentes.

On a donc la table suivante, avec ce contenu (commande ***nft list table inet filter***):

```
table inet filter {
	chain input {
		type filter hook input priority filter; policy accept;
	}

	chain output {
		type filter hook output priority filter; policy accept;
	}
}
```

Gestion des règles

Ajout de règles

Ajout d'une règle:

```
nft add rule filter input regle_a_appliquer
```

Par exemple pour ouvrir le port 80:

```
nft add rule filter input dport 80 accept
```

Et pour bloquer tout ce qui n'est pas explicitement écrit, on place cette règle à la fin, donc après avoir dénifie toutes nos règles:

```
nft add rule filter input drop
```

Pareil, si on veut bloquer tout le traffic sortant:

```
nft add rule filter output drop
```

Insertion de règles

Si on veut ajouter des règles, il va falloir les insèrer. En effet, l'ajout du drop, aura pour conséquence la non prise en compte des règles ajoutée après.
il faut donc passer par une intsertion de règles par rapport à celles déjà présentes.

Pour cela, il faut d'abor lister nos règles avec l'option -a:

```
root@debian:~# nft -a list table ip mon_filtreIPv4
table ip mon_filtreIPv4 { # handle 4
        chain input { # handle 1
        type filter hook input priority filter; policy accept;
        tcp dport 80 accept # handle 4
        drop # handle 5
    }

    chain output { # handle 3
        type filter hook output priority filter; policy accept;
        tcp sport 80 accept # handle 7
        drop # handle 8
    }
}
```

le "handle" correspond à l'identifant de la règle.

Donc si on veut ajouter une règle autorisant l'accès au port ssh:

```
nft add rule inet filter input position 4 tcp dport 22 accept
nft add rule inet filter output position 7 tcp sport 22 accept
```

La règle sera donc ajouter après position ciblée (ici 4 et 7).

Si on veut ajouter la règle avant la position ciblé, il faut juste faire un insert:

```
nft insert rule inet filter input position 4 tcp dport 22 accept
nft insert rule inet filter output position 7 tcp sport 22 accept
```

Suppression d'une règle

Pour supprimer une règle, il faudra utiliser le même principe que l'ajout, c'est à dire utiliser les handle (avec la command ***nft -a list***).

Par exemple pour supprimer la règle en position 7:

```
nft delete rule inet filter input handle 7
```

Sauvegarde des règles

La sauvegarde des règles de nftable est assez similaire à iptables.

On sauvegarde les règles existantes dans un fichier:

```
nft list table inet filter > nft_rules.rules
```

Les règles seront donc sauvegardées dans le fichier *nft_rules.rules*.

Pour restaurer les règles:

```
nft -f nft_rules.rules
```

Comme iptables, si on redémarre la machine, les règles ne sont pas persistantes.

Il faut soit faire un script qui se lance au démarrage et qui restaure nos règles avec "nft -f", soit ajouter la ligne suivante au fichier /etc/network/interface:

```
allow-hotplug ens192
iface ens192 inet static
        address 192.168.5.2/24
        gateway 192.168.5.254
        pre-up nft -f /etc/nftables/nft.fw
```

Ici nos règles sont dans le fichier /etc/nftables/nft.fw.

Cela ne marche que sur les systèmes sous debian.

Ressources:

→ Cours nftables IT-Connect

→ Get Started with nftables

→ Wiki nftables

Revision #3
Created 15 June 2023 08:27:25 by Lauris_Adm
Updated 15 June 2023 10:00:22 by Lauris_Adm