Distribution EOLE - Bac à idée #27993

era : "tous sauf" sur un port fait planté la génération des règles iptables

12/04/2019 17:21 - Emmanuel GARETTE

Statut:	Nouveau	**Début:**	12/04/2019
Priorité:	Normal	**Echéance:**	
Assigné à:		**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0.00 heure
Version cible:		**Temps passé:**	0.00 heure

Description

Je voulais interdire tous les accès à un serveur sauf le port 8500 avec era.

J'ai donc :

- démarré era ;
- cliquer sur la zone "pedago vers extérieur" (en vert) ;
- "ajouter" une nouvelle directive ;
- glisser/déposer le service ;
- cocher la case "tout sauf" à côté ;
- valider/valider/annuler/former/fichier enregistrer/fichier quitter ;
- bastion regen

```
root@amon:~# bastion regen

                      [ OK ]
 * Regénération des règles de pare-feu (modèle "3zones")iptables-restore: line 126 failed

                      [ OK ]
 * Mise en cache des règles de pare-feu
                      [ OK ]
 * Restauration des règles de pare-feu en cache
```

La règle iptables est :

```
iptables -A ext-ped ! -p tcp ! --dport 8500 -i enp0s3 -o enp0s9 -s 0/0 -d 0/0 -j DROP
```

Si je retire le 1er "!" la règle s'applique mais la règle n'est pas complète (Par contre ca n'interdit que TCP et pas les autres protocole).

Le mieux ca serait de faire une règle implicite qui interdit tout l'accès + un règle d'autorisation.

Historique

#1 - 18/04/2019 11:35 - Daniel Dehennin

La demande est très technique (trop?), je vais essayer de résumer le comportement voulu :

- Dans la zone **pédagogie** vers **extérieur**
- Pour un serveur source **serveur**
- Tu veux qu'il puisse initier une communication vers le port **TCP 8500** de n'importe quelle destination
- Tu veux lui interdire tout le reste en sortie

Cela veut dire qu'il faut générer deux règles :

```
-A ped-ext -s serveur -i ens6 -o ens4 -p tcp -m state --state NEW -m tcp --dport 8500 --tcp-flags SYN,RST,ACK
SYN -j ACCEPT
-A ped-ext -s serveur -i ens6 -o ens4 -m state --state NEW -j DROP
```

Il n’est pas possible de combiner une négation de protocole TCP avec l’argument **--dport** car en interne, le noyau appliquera le **--dport** à tous les protocols qui ne sont pas **tcp** et cela ne fonctionne pas pour **icmp** par exemple.

D’un point de vue technique, cela semble indiquer qu’il faut :

1. Construire une règle iptables avec les paramètres fournis par l’utilisateur et lui appliquer la politique de la zone (**ACCEPT** dans notre cas)
2. Construire une règles iptables avec les paramètres d’extrémités et lui appliquer la politique inverse de celle de la zone (**DROP** dans notre cas)

#2 - 10/09/2019 16:25 - Joël Cuissinat

- Tracker changé de Demande à Bac à idée