Distribution EOLE - Tâche #28738

Scénario # 28737 (Terminé (Sprint)): Traitement express MEN (27-35)

Bug dans la génération des règles iptables de log en cas de DNAT sur des ports différents

07/11/2019 04:32 PM - Laurent HAEFFELE

Status:	Fermé	**Start date:**	07/11/2019
Priority:	Normal	**Due date:**	
Assigned To:	Joël Cuissinat	**% Done:**	100%
Target version:	sprint 2019 27-35 Equipe MENSR (été)	**Estimated time:**	0.00 hour
		Spent time:	0.00 hour

Description

Nous avons sur certains établissements des règles de DNAT depuis l'extérieur vers des machines internes à l'établissement.
Les règles iptables générées par ERA ne sont pas correctes car la règles de LOG conserve le port initial alors que la règles d'autorisation utilise bien le port destination.
Par exemple si nous redirigeons les flux entrant sur le port 22222 du amon vers le port 3389 de la machine 10.168.253.221, cela va générer les règles suivantes :

```
/sbin/iptables -t nat -A PREROUTING -p tcp --dport 22222 --tcp-flags SYN,RST,ACK SYN -i eth0 -s A.B.C.D/255.255.255.255 -d 0.0.0.0/0.0.0.0 -j DNAT --to-destination 10.168.253.221:3389
/sbin/iptables -t filter -A ext-z1_ -p tcp --dport 22222 --tcp-flags SYN,RST,ACK SYN -i eth0 -o eth2 -s A.B.C.D/255.255.255.255 -d 10.168.253.221 -j LOG --log-prefix "iptables: era ext-bas"
/sbin/iptables -t filter -A ext-z1_ -p tcp --dport 3389 --tcp-flags SYN,RST,ACK SYN -i eth0 -o eth2 -s A.B.C.D/255.255.255.255 -d 10.168.253.221 -j ACCEPT
```

L'erreur se trouve dans la règle de log qui devrait être :

```
/sbin/iptables -t filter -A ext-z1_ -p tcp --dport 3389 --tcp-flags SYN,RST,ACK SYN -i eth0 -o eth2 -s A.B.C.D/255.255.255.255 -d 10.168.253.221 -j LOG --log-prefix "iptables: era ext-bas"
```

Associated revisions

Revision 67f233e0 - 07/16/2019 11:21 AM - Joël Cuissinat

NAT: log iptable rule dport must be the natted port

Otherwise the LOG --dport is the external opened port which can't match
in filter table.

- era/backend/processors.py (DNATDirectiveProcessor.process): move the "process_log()" call to use the natted "service_param2".

Ref: #28738

History

#1 - 07/12/2019 03:47 PM - Joël Cuissinat

Scénario pour reproduire une situation équivalente dans le contexte etb1.amon :

```
era -f /usr/share/era/modeles/4zones.xml
```

- exterieur->dmz
- Ajouter
  - Service : faire glisser un service avec port (ex : "8500")
  - Action : DNAT + faire glisser une extrémité DMZ (ex : serveur_scribe_dmz) + nouveau port : 3389
  - cocher journaliser
- Valider, tout fermer et enregistrer

Application :

```
bastion regen
iptables-save | grep -E "8500|3389"
```

Résultat :

```
-A PREROUTING -i ens4 -p tcp -m tcp --dport 8500 --tcp-flags SYN,RST,ACK SYN -j DNAT --to-destination 10.1.3.5
:3389
-A ext-dmz -d 10.1.3.5/32 -i ens4 -o ens7 -p tcp -m tcp --dport 8500 --tcp-flags SYN,RST,ACK SYN -j LOG --log-
prefix "iptables: era ext-dmz"
-A ext-dmz -d 10.1.3.5/32 -i ens4 -o ens7 -p tcp -m tcp --dport 3389 --tcp-flags SYN,RST,ACK SYN -j ACCEPT
```

#2 - 07/12/2019 05:12 PM - Joël Cuissinat

- Parent task set to #28737

#3 - 07/12/2019 05:24 PM - Joël Cuissinat

Grâce l'expérience à tâtons, j'obtiens un point d'entrée à la ligne 530 de era/backend/processors.py ...

#4 - 07/16/2019 10:10 AM - Joël Cuissinat

- Project changed from ERA to Distribution EOLE

- Status changed from Nouveau to En cours

#5 - 07/16/2019 10:10 AM - Joël Cuissinat

- Assigned To set to Joël Cuissinat

#6 - 07/16/2019 11:47 AM - Joël Cuissinat

Corrigé pour **EOLE>=2.6.1**

#7 - 07/16/2019 11:52 AM - Joël Cuissinat

- Status changed from En cours to Résolu

- % Done changed from 0 to 100

#8 - 08/21/2019 03:30 PM - Joël Cuissinat

- Status changed from Résolu to Fermé

- Remaining (hours) set to 0.0

Publié en stable le 20/08/2019.