eole-common - Anomalie #7171

firewall sur eolebase

01/22/2014 10:14 AM - Fabrice Barconnière

Status:	Fermé	**Start date:**	
Priority:	Normal	**Due date:**	03/21/2014
Assigned To:	Emmanuel GARETTE	**% Done:**	100%
Category:		**Estimated time:**	0.00 hour
Target version:	Eole 2.4-RC3	**Spent time:**	2.50 hours
Distribution:	EOLE 2.4		

Description

Dans le dico 01_network.xml on trouve ceci :

```
        <service_access service='sshd'>
            <port>22</port>
            <tcpwrapper>sshd</tcpwrapper>
        </service_access>
        <service_restriction service='sshd'>
            <ip interface='eth0' netmask='netmask_ssh_eth0' netmask_type='SymLinkOption' ip_type='
SymLinkOption'>ip_ssh_eth0</ip>
            <ip interface='eth1' netmask='netmask_ssh_eth1' netmask_type='SymLinkOption' ip_type='
SymLinkOption'>ip_ssh_eth1</ip>
            <ip interface='eth2' netmask='netmask_ssh_eth2' netmask_type='SymLinkOption' ip_type='
SymLinkOption'>ip_ssh_eth2</ip>
            <ip interface='eth3' netmask='netmask_ssh_eth3' netmask_type='SymLinkOption' ip_type='
SymLinkOption'>ip_ssh_eth3</ip>
            <ip interface='eth4' netmask='netmask_ssh_eth4' netmask_type='SymLinkOption' ip_type='
SymLinkOption'>ip_ssh_eth4</ip>
        </service_restriction>
```

Malgré ça aucune règle iptables associées n'est présente et /etc/hosts.allow n'est pas modifié en conséquence.

Related issues:

Related to eole-common - Anomalie #7144: eole-firewall sur Sphynx : erreur su...	**Fermé**		**01/24/2014**
Related to eole-common - Tâche #7698: eole-firewall bloque les conteneurs	**Fermé**	**03/19/2014**	**03/21/2014**

Associated revisions

Revision acc9915d - 01/22/2014 02:46 PM - Fabrice Barconnière

Remplacement d'un dico par une liste dans le template 50-nat_rules
Seule la dernière affectation accesses[clé] était prise en compte
fixes #7171 @2h

Revision cfd7e373 - 02/21/2014 03:30 PM - Emmanuel GARETTE

meilleur prise en compte des doublons (ref #7171)

History

#1 - 01/22/2014 11:55 AM - Fabrice Barconnière

Il semble que seule la dernière interface active soit traitée.

#2 - 01/22/2014 12:11 PM - Daniel Dehennin

J'ai testé sur un eolebase:

1. Installation d'un eolebase
2. Passer à **oui** la variable **Réseau avancé** -> **Activer le support du firewall**
3. Passer à **2** la variable **Général** -> **Nombre d'interfaces à activer**
4. Passer à **oui** la variable **Interface-0** -> **Autoriser les connexions pour administrer le serveur (EAD, phpMyAdmin, ...)**
5. Définir à **0.0.0.0** la variable **Interface-0** -> **Adresse IP réseau autorisée pour administrer le serveur**
6. Définir à **0.0.0.0** la variable **Interface-0** -> **Masque du sous réseau pour administrer le serveur**
7. Passer à **oui** la variable **Interface-1** -> **Autoriser les connexions pour administrer le serveur (EAD, phpMyAdmin, ...)**
8. Définir à **0.0.0.0** la variable **Interface-1** -> **Adresse IP réseau autorisée pour administrer le serveur**
9. Définir à **0.0.0.0** la variable **Interface-1** -> **Masque du sous réseau pour administrer le serveur**
10. Ajout d'une interface **eth1** (je n'avais qu'une interface physique)

```
root@eolebase:~# ip link add name eth1 type dummy
```

11. Instancier
12. Lister les règles iptables

```
root@eolebase:~# iptables -S
-P INPUT DROP
-P FORWARD DROP
-P OUTPUT ACCEPT
-N eth0-root
-N eth1-root
-A INPUT -i lo -j ACCEPT
-A INPUT -i eth0 -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -i eth0 -j eth0-root
-A INPUT -i eth1 -j eth1-root
-A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT
-A OUTPUT -o lo -j ACCEPT
-A eth0-root -p icmp -m icmp --icmp-type 3 -j ACCEPT
-A eth0-root -p icmp -m icmp --icmp-type 3/0 -j ACCEPT
-A eth0-root -p icmp -m icmp --icmp-type 4 -j ACCEPT
-A eth0-root -p icmp -m icmp --icmp-type 3/4 -j ACCEPT
-A eth0-root -p icmp -m icmp --icmp-type 11 -j ACCEPT
-A eth0-root -p icmp -m icmp --icmp-type 12 -j ACCEPT
-A eth0-root -p icmp -m icmp --icmp-type 0 -j ACCEPT
-A eth0-root -p icmp -m icmp --icmp-type 8 -j ACCEPT
-A eth0-root -m state --state RELATED,ESTABLISHED -j ACCEPT
-A eth0-root -j DROP
-A eth1-root -p icmp -m icmp --icmp-type 3 -j ACCEPT
-A eth1-root -p icmp -m icmp --icmp-type 3/0 -j ACCEPT
-A eth1-root -p icmp -m icmp --icmp-type 4 -j ACCEPT
-A eth1-root -p icmp -m icmp --icmp-type 3/4 -j ACCEPT
-A eth1-root -p icmp -m icmp --icmp-type 11 -j ACCEPT
-A eth1-root -p icmp -m icmp --icmp-type 12 -j ACCEPT
-A eth1-root -p icmp -m icmp --icmp-type 0 -j ACCEPT
-A eth1-root -p icmp -m icmp --icmp-type 8 -j ACCEPT
-A eth1-root -p udp -m udp --dport 514 -j ACCEPT
-A eth1-root -p tcp -m tcp --dport 4200 --tcp-flags FIN,SYN,RST,ACK SYN -j ACCEPT
-A eth1-root -p tcp -m tcp --dport 4201 --tcp-flags FIN,SYN,RST,ACK SYN -j ACCEPT
-A eth1-root -p tcp -m tcp --dport 4202 --tcp-flags FIN,SYN,RST,ACK SYN -j ACCEPT
-A eth1-root -p tcp -m tcp --dport 20514 --tcp-flags FIN,SYN,RST,ACK SYN -j ACCEPT
-A eth1-root -p tcp -m tcp --dport 10514 --tcp-flags FIN,SYN,RST,ACK SYN -j ACCEPT
-A eth1-root -p tcp -m tcp --dport 22 --tcp-flags FIN,SYN,RST,ACK SYN -j ACCEPT
-A eth1-root -p tcp -m tcp --dport 8090 --tcp-flags FIN,SYN,RST,ACK SYN -j ACCEPT
-A eth1-root -m state --state RELATED,ESTABLISHED -j ACCEPT
-A eth1-root -j DROP
```

Les règles ICMP sont appliquées sur toutes les interfaces mais pas les autres règles.

#3 - 01/22/2014 02:48 PM - Fabrice Barconnière

- Status changed from Nouveau to Résolu

- % Done changed from 0 to 100

Appliqué par commit eole-common:acc9915ded7bb7585899c0971e878047381cd84f.

#4 - 01/22/2014 05:50 PM - Emmanuel GARETTE

- Status changed from Résolu to À valider

- % Done changed from 100 to 80

Le but de ce dico était d'éviter d'avoir des règles de type "doublon" :

http://dev-eole.ac-dijon.fr/projects/eole-common/repository/revisions/57e0639e8c67627821ae3131c356c8b15c4b0ee2

Voir la partie "doublon" de la proposition de doc : http://dev-eole.ac-dijon.fr/issues/6313

La solution proposée à cette demande ne me semble pas pertinente. Il faudrait surement faire un dico de dico mais il faut mieux réfléchir à la solution proposée.

#5 - 01/23/2014 09:50 AM - Fabrice Barconnière

J'ai bien vu que le but d'avoir un dico était de ne pas avoir de règle en double, mais le choix de la clé n'était pas adapté.
Peut-être qu'un test de ce type pourrait éviter les doublons :

```
%if "nouvelle règle" not in %%accesses
    %%accesses.append("nouvelle règle")
```

#6 - 01/24/2014 09:34 AM - Joël Cuissinat

- Target version changed from Eole 2.4-RC1 to Eole 2.4-RC2

#7 - 02/17/2014 10:41 AM - Daniel Dehennin

- Target version changed from Eole 2.4-RC2 to Eole 2.4-RC3

#8 - 03/19/2014 12:21 PM - Daniel Dehennin

- Project changed from creole to eole-common

Tous les commits sont sur eole-common.

#9 - 03/24/2014 05:11 PM - Joël Cuissinat

- Due date set to 03/21/2014

- Status changed from À valider to Résolu

- Assigned To set to Emmanuel GARETTE

- % Done changed from 80 to 100

A été résolu.

#10 - 04/15/2014 03:58 PM - Emmanuel GARETTE

- Status changed from Résolu to Fermé

Règle existe bien.