

ERA - Anomalie #6478

Commentaires des règles dans lance.firewall

10/25/2013 10:56 AM - Jean-Marc MELET

Status:	Fermé	Start date:	
Priority:	Bas	Due date:	11/08/2013
Assigned To:	Gwenael Remond	% Done:	100%
Category:		Estimated time:	0.00 hour
Target version:	Mises à jour 2.3.11	Spent time:	0.17 hour
Distribution:	EOLE 2.3		

Description

Ceci est juste un problème cosmétique d'affichage des commentaires dans la génération de lance.firewall.

Lorsqu'on édite le fichier, il apparaît plusieurs règles citées en dessous du commentaire "Paquets contenant la zone pubdmz" mais qui ne concernent pas cette zone (par ex des règles ped-pri et pri-ped):

```
## Paquets contenant la zone pubdmz
/sbin/iptables -t filter -A pub-ext -i eth4 -o eth0 -s 0/0 -d 0/0 -j ACCEPT
/sbin/iptables -t filter -A ext-pub -i eth0 -o eth4 -s 0/0 -d 0/0 -j DROP
/sbin/iptables -t filter -A adm-pub -i eth1 -o eth4 -s 0/0 -d 0/0 -j ACCEPT
/sbin/iptables -t filter -A pub-adm -i eth4 -o eth1 -s 0/0 -d 0/0 -j DROP
/sbin/iptables -t filter -A pub-bas -i eth4 -s 0/0 -d 0/0 -j DROP
/sbin/iptables -t filter -A ped-pri -i eth2 -o eth3 -s 0/0 -d 0/0 -j ACCEPT
/sbin/iptables -t filter -A pri-ped -i eth3 -o eth2 -s 0/0 -d 0/0 -j DROP
/sbin/iptables -t filter -A ped-pub -i eth2 -o eth4 -s 0/0 -d 0/0 -j ACCEPT
/sbin/iptables -t filter -A pub-ped -i eth4 -o eth2 -s 0/0 -d 0/0 -j DROP
/sbin/iptables -t filter -A pri-pub -i eth3 -o eth4 -s 0/0 -d 0/0 -j ACCEPT
/sbin/iptables -t filter -A pub-pri -i eth4 -o eth3 -s 0/0 -d 0/0 -j DROP
```

D'autre part, le classement des règles concernant les redirections pour wpad n'est pas clair. L'ensemble des règles concernées pour les zones admin et peda sont affichées dans plusieurs sections de commentaires:

```
### Redirection des flux vers le serveur de distribution du fichier wpad
/sbin/iptables -t filter -A adm-bas -i eth1 -p tcp --dport 81 -j ACCEPT
/sbin/iptables -t nat -A PREROUTING -p tcp --dport 80 --tcp-flags SYN,RST,ACK SYN -i eth1 -s 0/0 -
d 0/0 -j REDIRECT --to-ports 81
/sbin/iptables -t nat -A PREROUTING -p tcp --dport 3128 --tcp-flags SYN,RST,ACK SYN -i eth1 -s 0/0
-d 0/0 -j REDIRECT --to-ports 81
/sbin/iptables -t nat -A PREROUTING -p tcp --dport 8080 --tcp-flags SYN,RST,ACK SYN -i eth1 -s 0/0
-d 0/0 -j REDIRECT --to-ports 81
## Regles montantes entre <zone:bastion> et <zone:admin>
### Redirection pour le fichier wpad.
/sbin/iptables -t nat -A PREROUTING -p tcp --dport 80 --tcp-flags SYN,RST,ACK SYN -i eth1 -s 0/0 -
d 10.13.31.125 -j REDIRECT --to-ports 81
## Regles montantes entre <zone:bastion> et <zone:pedago>
/sbin/iptables -t nat -A PREROUTING -p tcp --dport 80 --tcp-flags SYN,RST,ACK SYN -i eth2 -s 0/0 -
d 172.20.247.245 -j REDIRECT --to-ports 81
### pedago -> exterieur : tout interdire (sauf le web via le proxy) : INACTIVE
/sbin/iptables -t filter -A ped-bas -i eth2 -p tcp --dport 81 -j ACCEPT
/sbin/iptables -t nat -A PREROUTING -p tcp --dport 80 --tcp-flags SYN,RST,ACK SYN -i eth2 -s 0/0 -
d 0/0 -j REDIRECT --to-ports 81
/sbin/iptables -t nat -A PREROUTING -p tcp --dport 3128 --tcp-flags SYN,RST,ACK SYN -i eth2 -s 0/0
-d 0/0 -j REDIRECT --to-ports 81
/sbin/iptables -t nat -A PREROUTING -p tcp --dport 8080 --tcp-flags SYN,RST,ACK SYN -i eth2 -s 0/0
-d 0/0 -j REDIRECT --to-ports 81
```

Associated revisions

Revision 84125aab - 11/04/2013 02:27 PM - Gwenael Remond

ajout des commentaires, fixes #6478

Revision 18327671 - 11/04/2013 02:30 PM - Gwenael Remond

ajout des commentaires, fixes #6478

History

#1 - 10/31/2013 08:59 AM - Gwenael Remond

dans le cas des règles "## Paquets contenant la zone" je n'arrive pas à reproduire ce bug sur les commentaires.
je ne vois pas dans le code ce qui pourrait provoquer un tel bug.
quel modèle utilises-tu ? quelle version d'Era ?

#2 - 10/31/2013 09:54 AM - Gwenael Remond

ah. si c bon, j'ai reproduit...

#3 - 11/04/2013 02:27 PM - Gwenael Remond

- Status changed from *Nouveau* to *Résolu*
- % Done changed from 0 to 100

Appliqué par commit [84125aaba377e888e5bfe60397dbb8c16bcf8a1f](#).

#4 - 11/04/2013 02:30 PM - Gwenael Remond

Appliqué par commit [18327671b74a1f1aab97132349f1e95720d92cde](#).

#5 - 11/04/2013 02:40 PM - Gwenael Remond

en ce qui concerne le classement des règles wpad, pour l'instant pas grand chose à faire, ça ne peut pas être réordonné car ce qui concerne wpad est dans deux directives (au sens Era, dans l'interface) séparées, donc les directives étant différentes, la génération se fera à deux endroits différents.

Pouvoir réorganiser les directives et les règles en fonctions d'un thème donné n'est pas encore une fonctionnalité implémentée dans Era (et ça ferait l'objet d'une release majeure)

#6 - 11/04/2013 03:42 PM - Gwenael Remond

- Assigned To set to *Gwenael Remond*
- Distribution changed from *EOLE 2.3* to *Toutes*

#7 - 11/06/2013 11:29 AM - Fabrice Barconnière

- Due date set to *11/08/2013*
- Target version set to *Mises à jour 2.3.11*
- Distribution changed from *Toutes* to *EOLE 2.3*

#8 - 11/20/2013 03:30 PM - Fabrice Barconnière

- Status changed from *Résolu* to *Fermé*

OK pour la première partie de la demande.
La 2ème partie n'a pu être traitée car elle nécessite un peu plus que du développement d'ERA.