Distribution EOLE - Tâche #36838

Scénario # 36031 (Terminé (Sprint)): EOLE 2.10 : gestion du netfilter conntrack helper

Etude

06/05/2025 14:44 - Emmanuel GARETTE

Statut:	Fermé	**Début:**	06/05/2025
Priorité:	Normal	**Echéance:**	
Assigné à:	Emmanuel GARETTE	**% réalisé:**	100%
Version cible:	Livraison Cadoles - MEN 30/06/2025 (20)	**Temps estimé:**	0.00 heure
		Temps passé:	0.00 heure

Description

Historique

#1 - 20/05/2025 10:10 - Emmanuel GARETTE

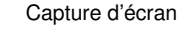
- Fichier Capture d'écran du 2025-05-20 09-07-32.png ajouté

Support des helper sur Amon

Depuis l'*extérieur*, pour accéder au service FTP, SIP, H.323, ... (sur EOLE on utilise "FTP" et "TFTP" par défaut).

Pour une directive particulière (FTP, ...), il faut maintenant définir le helper associé.

Il est possible d'ajouter un champs dans l'onglet service (un peut comme tcpwrapper) :


Capture d'écran du 2025-05-20 09-07-32.png

Ensuite il faut enregistrer l'information dans le fichier (donc changer le format du fichier XML en 2.10).

Enfin, si une directive contient un service qui a un "helper", il faut généré un règle implicite à partir de cette information.

Il est donc nécessaire :

- de supprimer le chargement des modules pour FTP et TFTP ;
- de modifier le frontend GTK pour ajouter le champs et le sauvegarder ;
- de modifier le générateur de règles iptables ;
- de revoir la documentation de Era.

Support des HELPER sur Scribe

Depuis l'*intérieur* et l'*extérieur* il faut autorisé l'accès au FTP :

```
iptables -I PREROUTING -t raw -p tcp --dport 21 -j CT --helper ftp
iptables -A INPUT -m conntrack --ctstate RELATED -m helper --helper ftp -p tcp --dport 1024: -j ACCEPT
```

Il faut adapter la règle pour définir la source et/ou la destination.

Ces règles peuvent être mise dans le template "11-proftpd".

Deux points d'attention annexe :

- quand je fais un "bastion regen" j'ai les erreurs suivantes :

```
 * Regénération des règles de pare-feuERRO[0000] tearing down network namespace configuration for container a2
f1289cf2e6e74c40e9508615af633208764946c5021696e5dee14ec7ff5cf7: netavark: code: 1, msg: iptables: No chain/tar
get/match by that name.
```

- la règle de pré routing n'est pas supprimé :

```
root@scribe:~# iptables-save|grep helper
-A PREROUTING -p tcp -m tcp --dport 21 -j CT --helper ftp
-A INPUT -p tcp -m conntrack --ctstate RELATED -m helper --helper ftp -m tcp --dport 1024:65535 -j ACCEPT
root@scribe:~# bastion regen


           [ OK ]
 * Regénération des règles de pare-feuERRO[0000] tearing down network namespace configuration for container a2
f1289cf2e6e74c40e9508615af633208764946c5021696e5dee14ec7ff5cf7: netavark: code: 1, msg: iptables: No chain/tar
get/match by that name.


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

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

                  ERRO[0000] tearing down network namespace configuration for container a2f1289cf2e6e74c40e950
8615af633208764946c5021696e5dee14ec7ff5cf7: netavark: code: 1, msg: iptables: No chain/target/match by that na
me.


           [ OK ]
root@scribe:~# iptables-save|grep helper
-A PREROUTING -p tcp -m tcp --dport 21 -j CT --helper ftp
```

#2 - 20/05/2025 16:16 - Emmanuel GARETTE

- Statut changé de Nouveau à À valider

- Assigné à mis à Emmanuel GARETTE

- % réalisé changé de 0 à 100

#3 - 22/09/2025 15:00 - Laurent Gourvenec

- Statut changé de À valider à Résolu

#4 - 22/09/2025 16:47 - Joël Cuissinat

- Statut changé de Résolu à Fermé

- Restant à faire (heures) mis à 0.0

Fichiers

Capture d'écran du 2025-05-20 09-07-32.png	78,1 ko	20/05/2025	Emmanuel GARETTE