Era

Présentation et nouvelles fonctionnalités

gwen

18 octobre 2012

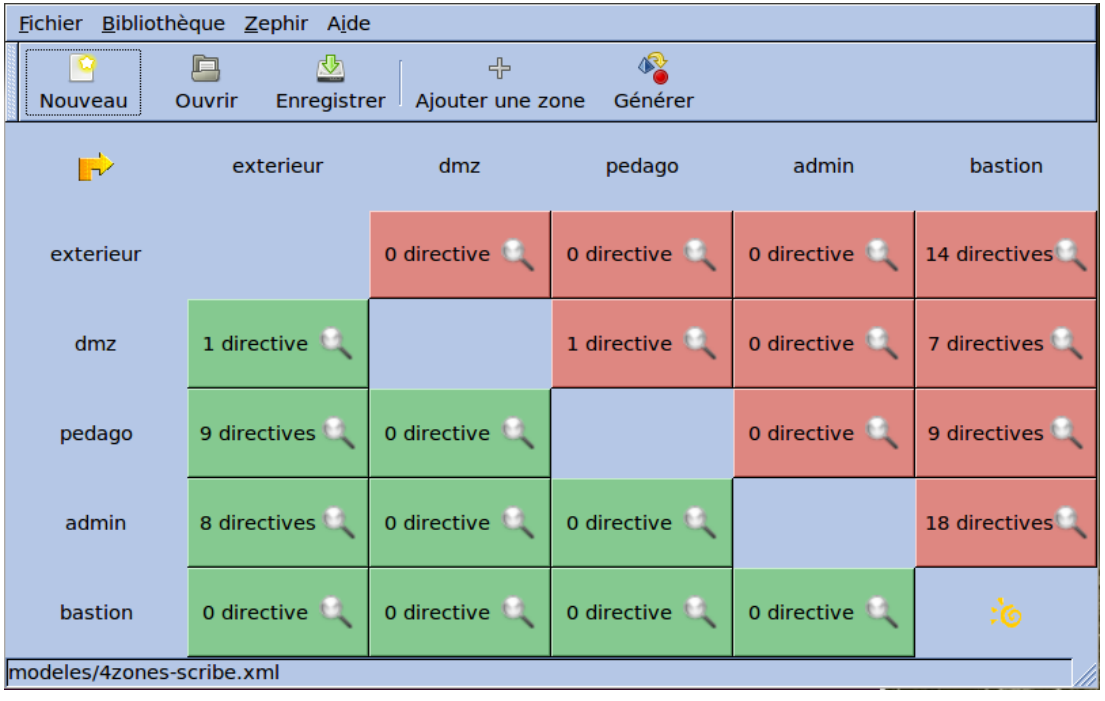
Ministère de l'Écologie, du Développement durable et de l'Énergie

Cadoles

ministère éducation nationale

Rappels

- un éditeur de politique de sécurité



- collecter et de centraliser des directives de securité
- un compilateur de règles
- un logiciel qui a plus de dix ans

Ministère de l'Écologie, du Développement durable et de l'Énergie

Cadoles

ministère éducation nationale

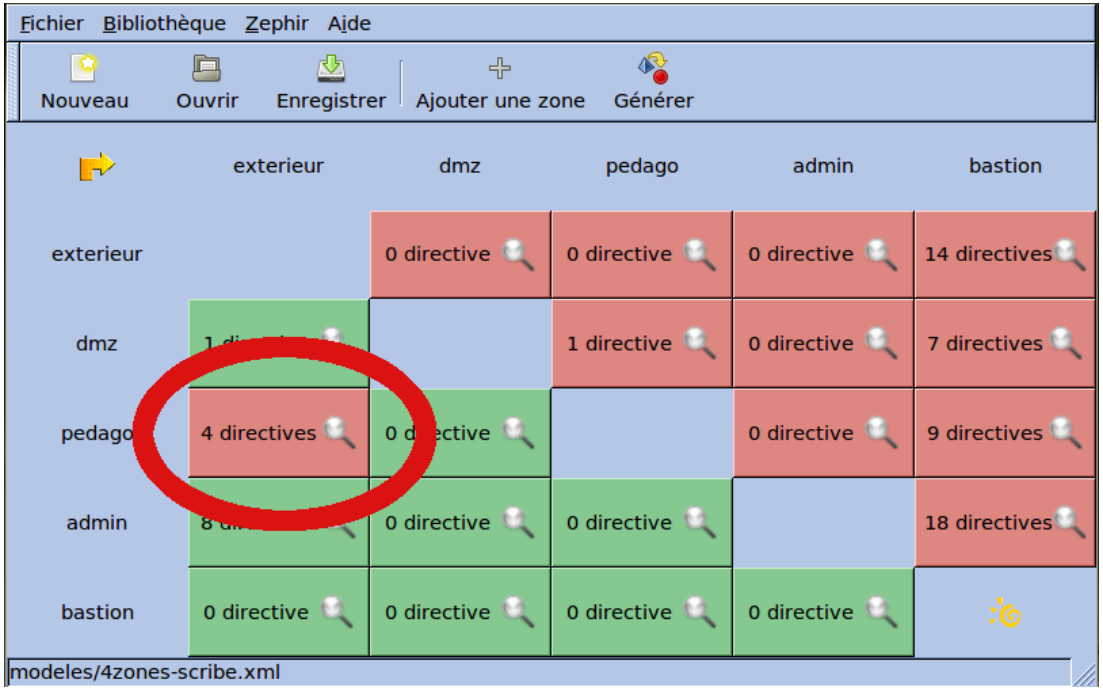
Le générateur de règles

Les directives de sécurité génèrent des ensembles de règles de bas niveau

- principalement de l'`iptables`, mais aussi :
- `tc` (`QOS`)
- de l'`ipsets` (cf slides suivantes)
- de l'iptables avec une ipsec policy
- d'autres syntaxes existent mais sont peu utilisées

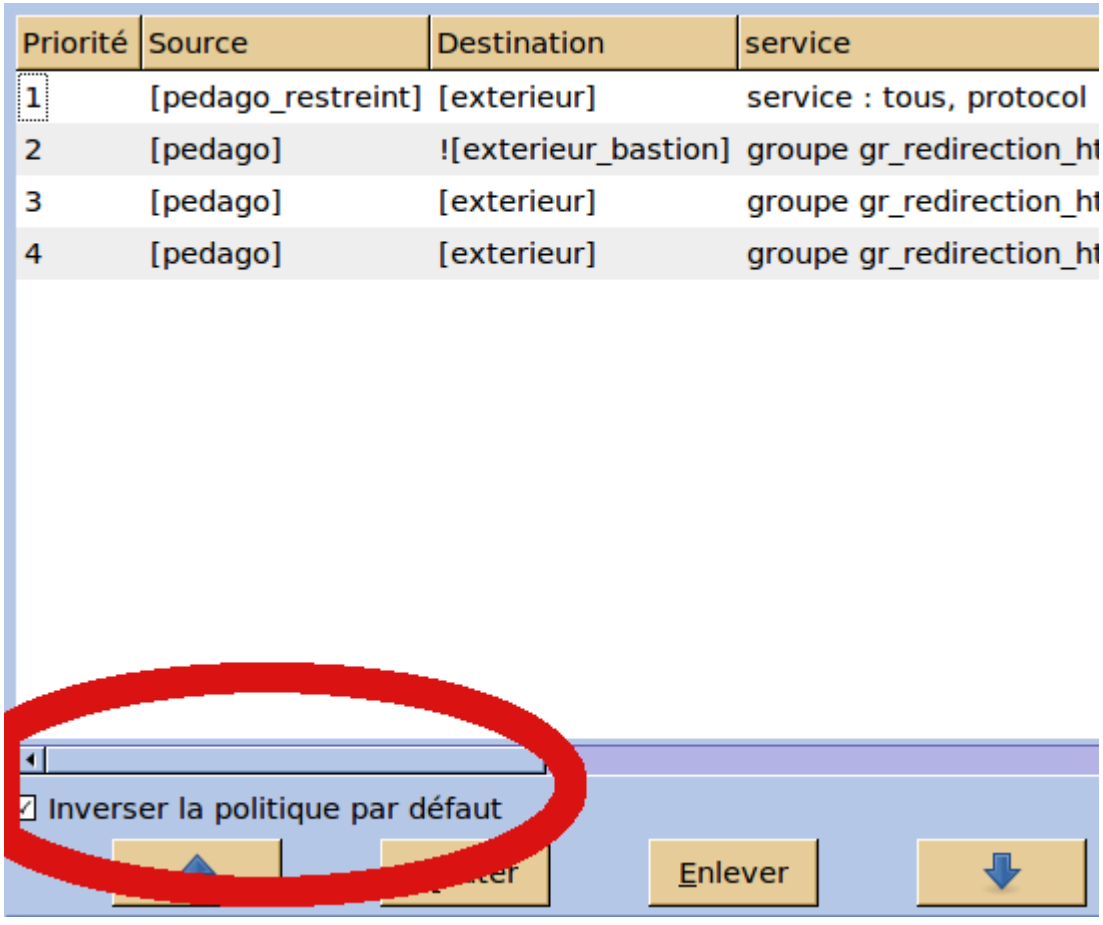
outil de conception

- conception autour des cartes physiques du pare-feu
- une politique par défaut (rappelons qu'elle est inversible :)



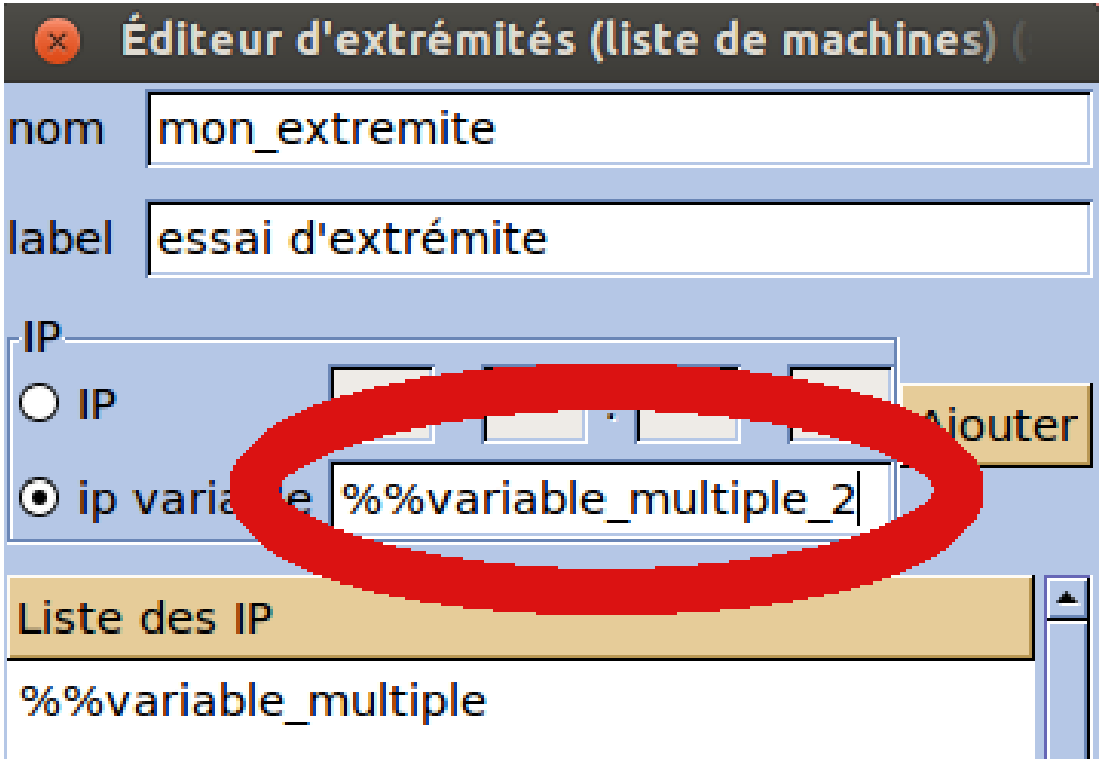
inversion de la politique par défaut

- comment inverser la politique par défaut dans un flux



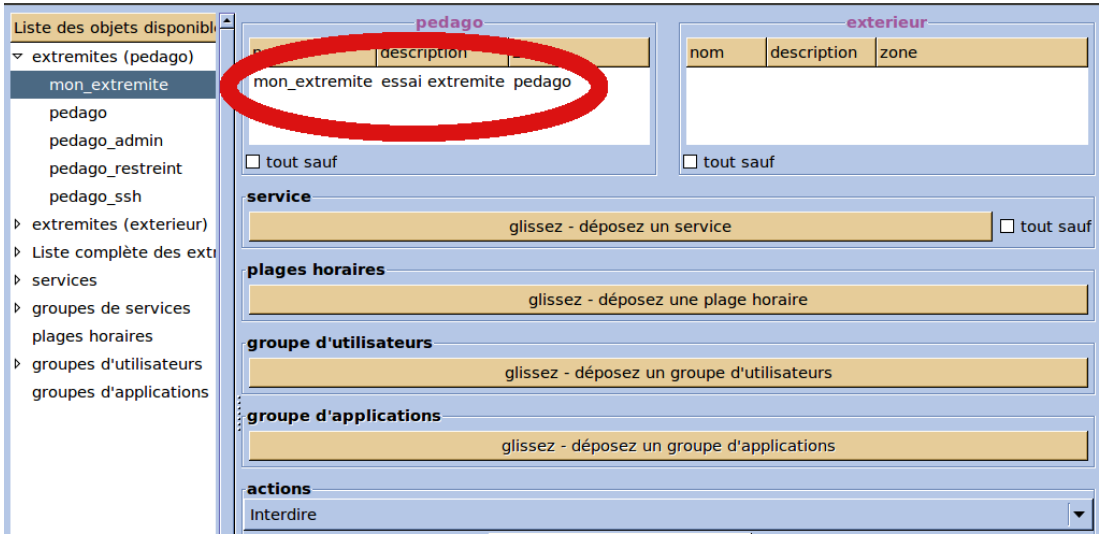
nouvelle fonctionnalité : intégration Créole

- il est possible depuis le début d'utiliser des variables Créole
- il est possible maintenant d'utiliser des variables Créole *multiples*



nouvelle fonctionnalité : intégration Créole (2)

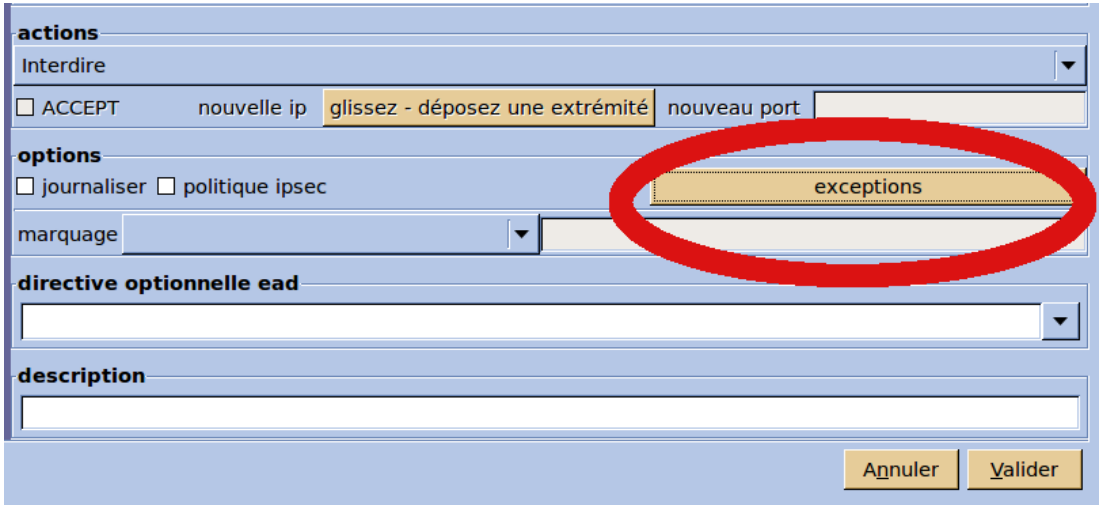
- utilisation de la syntaxe Créole et des variables multi-valuées dans les inclusions statiques
- et un peu partout dans l'interface :



nouvelle fonctionnalité : exceptions d'une directive

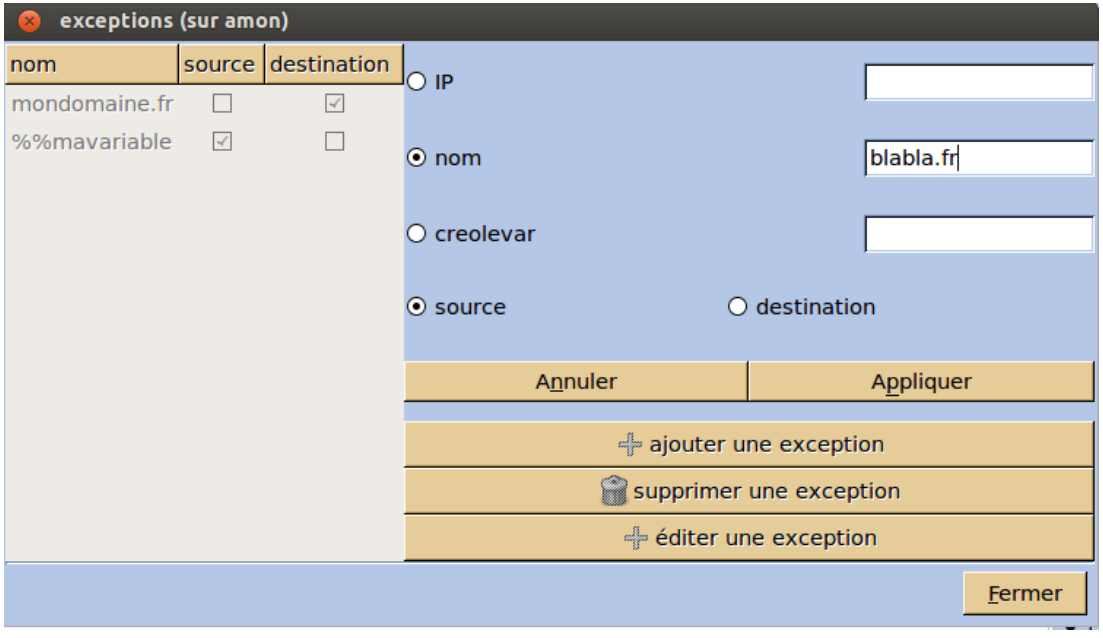
à ne pas confondre avec les "tout sauf" : les exceptions.
Uniquement pour les directives de type :

- interdiction,
- autorisation,
- redirection.
- pas pour le DNAT ou le SNAT (pas de sens)



nouvelle fonctionnalité : exceptions d'une directive (2)

La fenêtre d'édition des exceptions :



(la variable Créole peut bien sûr être une multi)

eole-firewall

- eole-firewall est conçu pour gérer les flux réseau d'un module EOLE, il peut-être utilisé en complément d'Era ou de façon indépendante
- eole-firewall ne gère que des "autorisations"
- utilisé en complément d'Era, il gère uniquement les connexions entre les conteneurs, des conteneurs vers le maître et des conteneurs vers l'extérieur,
- tous les flux entre zones sont alors gérés par Era.

perspectives et développements

- meilleure centralisation des directives de sécurité par des "plug-ins" associés à différents modules
- Era pourrait ainsi s'occuper de plusieurs modules plutôt que (il est cantoné historiquement Amon)
- prise en charge des conteneurs (intégration complète de eole-firewall dans Era)
- se recentrer sur le but de l'outil (intégration et centralisation des règles de sécurité)