

Era

Présentation et nouvelles fonctionnalités

gwen



18 octobre 2012

Cadole

► un éditeur de politique de sécurité

	exterieur	dmz	pedago	admin	bastion
exterieur		0 directive	0 directive	0 directive	14 directives
dmz	1 directive		1 directive	0 directive	7 directives
pedago	9 directives	0 directive		0 directive	9 directives
admin	8 directives	0 directive	0 directive		18 directives
bastion	0 directive	0 directive	0 directive	0 directive	

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

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 :)

The screenshot shows a software interface for configuring firewall policies. The menu bar includes 'Fichier', 'Bibliothèque', 'Zephir', and 'Aide'. The toolbar contains 'Nouveau', 'Ouvrir', 'Enregistrer', 'Ajouter une zone', and 'Générer'. The main area displays a matrix of policies between five zones: exterieur, dmz, pedago, admin, and bastion. The matrix cells show the number of directives and a magnifying glass icon. A red circle highlights the cell for the policy between 'pedago' and 'exterieur', which contains '4 directives'.

	exterieur	dmz	pedago	admin	bastion
exterieur		0 directive	0 directive	0 directive	14 directives
dmz	1 directive		1 directive	0 directive	7 directives
pedago	4 directives	0 directive		0 directive	9 directives
admin	8 directives	0 directive	0 directive		18 directives
bastion	0 directive	0 directive	0 directive	0 directive	

inversion de la politique par défaut

- ▶ comment inverser la politique par défaut dans un flux

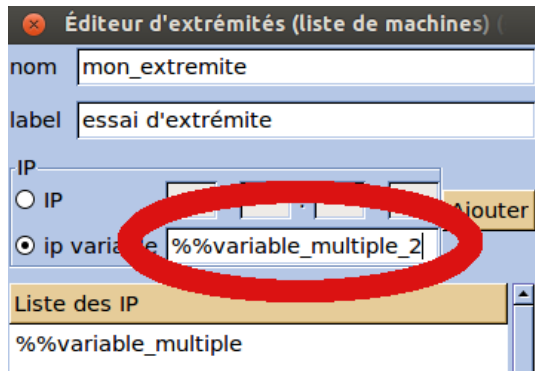
Priorité	Source	Destination	service
1	[pedago_restreint]	[exterieur]	service : tous, protocol
2	[pedago]	![exterieur_bastion]	groupe gr_redirection_ht
3	[pedago]	[exterieur]	groupe gr_redirection_ht
4	[pedago]	[exterieur]	groupe gr_redirection_ht

Inverser la politique par défaut

↑ Enlever ↓

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 :

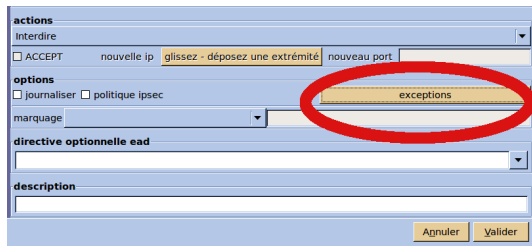
The screenshot shows the 'Liste des objets disponibles' (List of available objects) interface. On the left, a tree view lists various object categories like 'extremites (pedago)', 'extremites (exterieur)', 'services', etc. The main area displays a table with columns 'nom', 'description', and 'zone'. A red circle highlights the row with 'mon_extremite' in the 'nom' column and 'essai extremite pedago' in the 'description' column. Below the table, there are sections for 'service', 'plages horaires', 'groupe d'utilisateurs', 'groupe d'applications', and 'actions'.

pedago		exterieur		
nom	description	nom	description	zone
mon_extremite	essai extremite pedago			

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)



The screenshot shows a configuration window with the following sections:

- actions**: A dropdown menu set to "Interdire". Below it, there are input fields for "nouvelle ip" (containing "glissez - déposez une extrémité") and "nouveau port".
- options**: A checkbox for "journaliser" and a checkbox for "politique ipsec". A button labeled "exceptions" is highlighted with a red circle.
- marquage**: A dropdown menu.
- directive optionnelle ead**: A dropdown menu.
- description**: A text input field.
- Buttons for "Annuler" and "Valider" at the bottom right.

nouvelle fonctionnalité : exceptions d'une directive (2)

La fenêtre d'édition des exceptions :

nom	source	destination
mondomaine.fr	<input type="checkbox"/>	<input checked="" type="checkbox"/>
%mavariabile	<input checked="" type="checkbox"/>	<input type="checkbox"/>

IP

nom

creolevar

source destination

Annuler Appliquer

+ ajouter une exception

supprimer une exception

+ éditer une exception

Fermer

(la variable Créole peut bien sûr être une multi)

- ▶ 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.

- ▶ 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 cantonné 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)