

J-EOLE 10-11 Juin 2015

ERA

Présentation et nouvelles fonctionnalités

Gwenaël Rémond (Gwen)

CC BY-NC-SA 2.0 FR

ERA – Présentation et Nouveautés

Rappels :

- **ERA** est :
 - Un éditeur de politique de sécurité
 - Un compilateur de directives de sécurité

ERA – Présentation et Nouveautés

Fichier Bibliothèque Zephir Aide

Nouveau Ouvrir Enregistrer Ajouter une zone Générer

	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 🔍	🔧

modeles/4zones-scribe.xml

ERA – Présentation et Nouveautés

Le générateur de règles de sécurité

Des ensembles de règles de bas niveau sont générés, principalement de l'iptables, mais aussi de l'ipset, du tc (pour la QOS)...

ERA – Présentation et Nouveautés

Peu de changements de bas niveau (impactant le compilateur de règles)

- suppression de eole-firewall et prise en compte de la gestion des conteneurs
 - la syntaxe ipset a un peu changé (création d'ipset de type 'net' plutôt que 'IP')

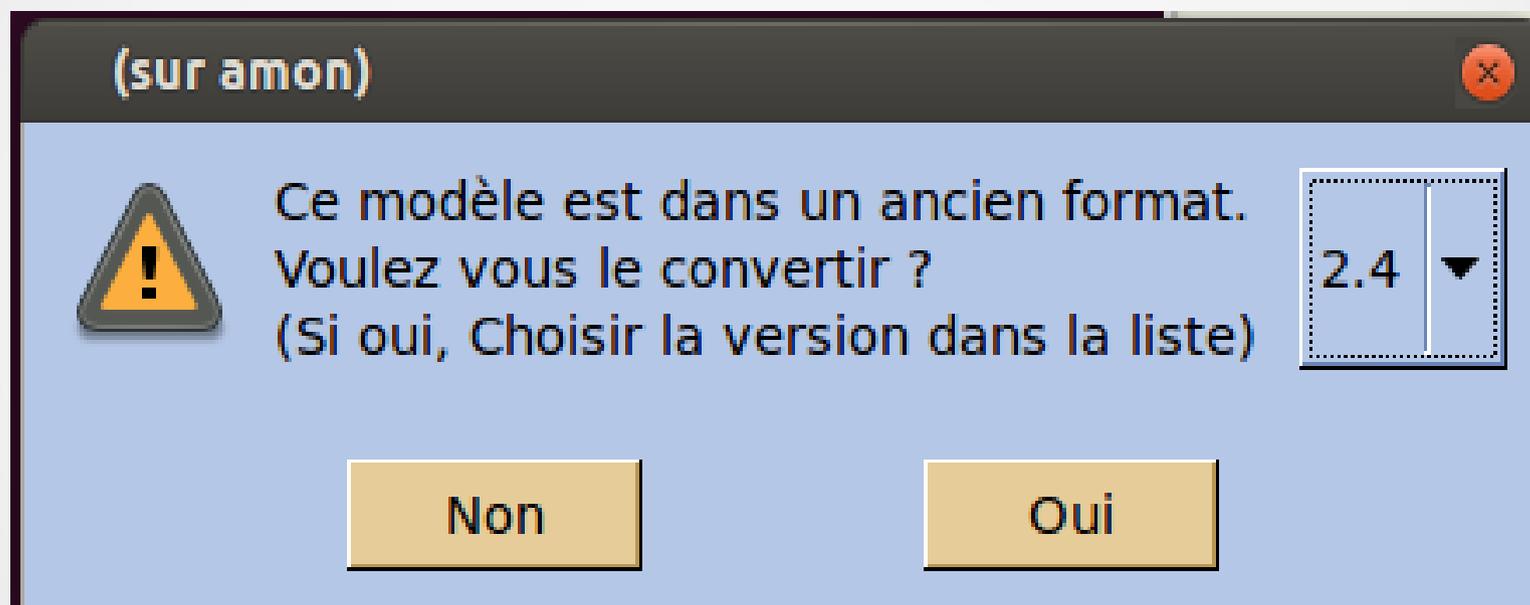
ERA – Présentation et Nouveautés

Changements dans la DTD du format XML interne à l'application : La version XML 2.4

Script de migration fourni pour passer en 2.4
<firewall version="2.4">

Pas de lien avec le versioning EOLE !

ERA – Présentation et Nouveautés



ERA – Présentation et Nouveautés

Le typage des extrémités

Les extrémités sont maintenant typées
(`'normal'`, `'conteneur'`, `'alias'`)

ERA – Présentation et Nouveautés

Éditeur d'extrémités (liste de machines) (sur amc) ✕

nom

label

IP

IP . . .

ip variable

Liste des IP

Type normal

ERA – Présentation et Nouveautés

Le mode conteneur

On peut ajouter des extrémités de type 'conteneur' dans la zone 'bastion'

ERA – Présentation et Nouveautés

Éditeur d'extrémités (liste de machines) (su 

nom

label

IP

IP . . .

ip variable

Liste des IP

Type

Interface

container name

ERA – Présentation et Nouveautés

Éditeur d'extrémités (liste de machines) (su ✕)

nom

label

IP

IP . . .

ip variable

Liste des IP

Type	alias
------	-------

ERA – Présentation et Nouveautés

Les changements dans le support de l'héritage des modèles XML

L'inversion de la politique par défaut

Le passage des options du modèles

Les inclusions statiques

L'héritage de la QOS

ERA – Présentation et Nouveautés

Fichier Bibliothèque Zephyr Aide

Nouveau Ouvrir Enregistrer Ajouter une zone Générer

	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 🔍	

modeles/4zones-scribe.xml

ERA – Présentation et Nouveautés

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 ↓

ERA – Présentation et Nouveautés

TCPwrapper

implémenter un service avec tcpwrapper

Bibliothèque > services > liste des services

ERA – Présentation et Nouveautés

Éditeur de services (sur amonecole)

nom du service

description

protocole

protocole ▼

protocole variable

ports

port de à

ports de à



Licence

Cette présentation est mise à disposition sous licence
Creative Commons by-nc-sa 2.0-fr

Attribution	Partage dans les mêmes conditions
Pas d'utilisation commerciale	France

Vous pouvez obtenir une copie de la licence :

– Par internet :

<https://creativecommons.org/licenses/by-nc-sa/2.0/fr/>

– Par courrier postal : Creative Commons, 444 Castro Street,
Suite 900 Mountain View, California, 94041, USA