






















*Séminaire*

*22-23 Novembre 2006*

# ERA

## Editeur de Regles pour Amon

	 Nouveau	 Ouvrir	 Enregistrer	 Ajouter une zone	 Générer
	exterieur	pedago	admin	bastion	
exterieur		0 directives 	0 directives 	3 directives 	
pedago	10 directives 		0 directives 	7 directives 	
admin	2 directives 	0 directives 		5 directives 	
bastion	0 directives 	0 directives 	0 directives 		





# application graphique de génération de règles de sécurité

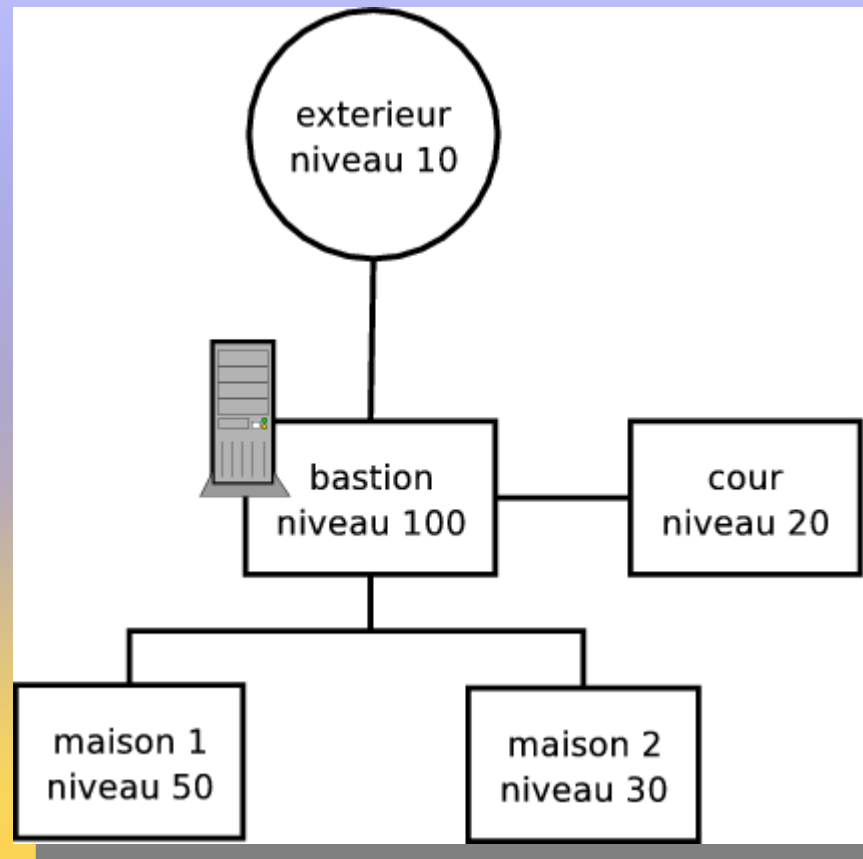
Era se compose de deux parties :

- l'editeur de pare-feu  
organise la politique de filtrage  
et l'enregistre dans un fichier XML.
- le générateur de règles iptables  
produit le script iptables à partir du fichier XML.



# conception d'un pare-feu


une modélisation préalable  
du pare-feu permet d'ordonner des zones  
pour une cohérence globale de sécurité



# le modèle de sécurité

chaque zone est reliée à une autre zone par des flux

- les flux montants
  - les flux descendants
- correspondent à
- des interdictions
  - des autorisations

	Gest	Ped	Ext
Gest		Autorisé	Autorisé
Ped	Interdit		Autorisé
Ext	Interdit	Interdit	





# les types de directives

fonctionnalités associées à chaque directive

- plages horaires
- logs
- directives implicites
- autorisation
- interdiction
- redirection
- snat, dnat



# era et amon

utilisation des variables  
de dictionnaire créole  
dans des extrémités  
ou des zones

Informations relatives à la zone

Nom

Niveau : 10

IP

IP  .  .  .

ip variable

Adresse du réseau  .  .  .

network variable

Masque du réseau  .  .  .

netmask variable

Interface  ▼



# era et amon (2)

activer ou désactiver des directives optionnelles depuis l'ead

## Gestion des règles du pare-feu

### pare-feu-3cartes

description	actif	inactif
interdire l'utilisation des dialogues en direct (icq)	<input type="radio"/>	<input checked="" type="radio"/>
interdire l'utilisation du pop, de l'imap et du smtp	<input checked="" type="radio"/>	<input type="radio"/>
interdire l'utilisation du transfert de fichiers	<input checked="" type="radio"/>	<input type="radio"/>
interdire l'utilisation des forums	<input type="radio"/>	<input checked="" type="radio"/>
on ferme tout sauf l'utilisation du web par le proxy	<input type="radio"/>	<input checked="" type="radio"/>
		<input type="button" value="Valider"/>

## Navigation

### home

page d'accueil

### services

page des services

### règles du pare-feu

gestion des règles du pare-feu

### accès réseau

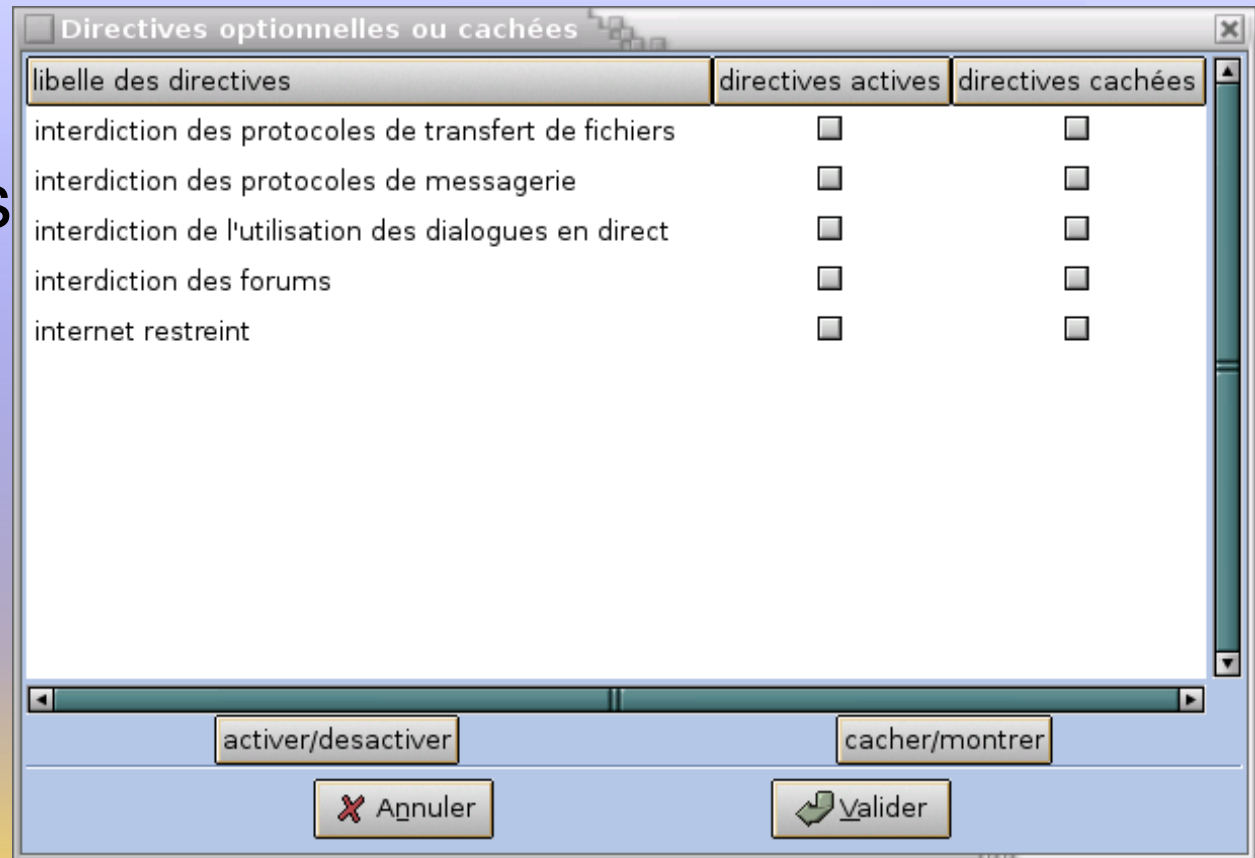
gestion de l'accès réseau pour les postes clients

### gestion p2p



# era et amon (3) directives cachées

utilisation des variables  
de dictionnaire créole  
pour conditionner  
des directives cachées





Merci de votre attention.

