Séminaire EOLE
Dijon
20-21 Octobre 2008

Filtrage sur Amon

Principes

Amon utilise des filtres

Un filtre peut être attaché à plusieurs interfaces

Une interface réseau est rattachée à un filtre

- Les connexions des stations en dehors de leur zone sont filtrées

Chaque filtre est configuré indépendamment

Délégation des droits d'administration d'un filtre

Fonctionnalités

Différents types de filtrage Web

Filtrage Web par utilisateurs

Groupes de machines

Fonctionnalités

Règles de pare-feu

Antivirus web

Filtrage de protocoles (L7filter)

Différents types de filtrage

- Blacklists
  - Base « adulte » non-désactivable
  - Activation de listes optionnelles
- Par extensions
- Par types MIME
- Filtrage syntaxique des pages

Les groupes de machines

ACTIVATION DES FILTRES FACULTATIFS SUR LA ZONE DE CONFIGURATION 1

- Filtres
- Filtrage
- Sites interdits
- Sites autorisés
- Extensions
- Type MIME
- Sites du mode liste blanche

FILTRES	DÉFAUT	1	2	3
	tous aucun	tous aucun	tous aucun	tous aucun
contenus agressifs (xenophobie...)	☐	☐	☐	☐
audio/video	☐	☐	☐	☐
téléphones mobiles, sonneries	☐	☐	☐	☐
radios en ligne	☐	☐	☐	☐
drogue	☐	☐	☐	☐
mail et chat	☐	☐	☐	☐
webmail les plus connus	☐	☐	☐	☐
jeux de hasard et d'argent	☐	☐	☐	☐
jeux en ligne	☐	☐	☐	☐
hacking (piratage)	☐	☐	☐	☐
phishing	☐	☐	☐	☐
warez (piratage)	☐	☐	☐	☐
triche aux examens	☐	☐	☐	☐
bandeaux publicitaires	☐	☐	☐	☐
divers (humour...)	☐	☐	☐	☐
utilisation de proxy distants	☐	☐	☐	☐
proxy spécifiques	☐	☐	☐	☐

[✓ Valider]

Filtrage Web utilisateurs

Ne fonctionne que si l'authentification proxy est activée

Un utilisateur est associé à une politique de filtrage

Politiques intégrées :

- Par défaut
- Modérateurs
- Utilisateurs interdits
- Mode liste blanche « *tout interdit sauf* »

4 politiques optionnelles activables

Filtrage Web utilisateurs

GESTION DES UTILISATEURS SUR LA ZONE DE CONFIGURATION 2

Login de l'utilisateur à gérer sur la zone de configuration 2

[Valider]

Modérateurs | Utilisateurs interdits | Utilisateurs en mode liste blanche

Login des utilisateurs	politique de filtrage	suppression
admin	modérateur	✗
cpe	1	✗
invite	liste blanche	✗
jean.bonnot	modérateur	✗
stagiaire_puni	interdits	✗

Les groupes de machines

Définis par plages d'adresses

Interdiction du surf :

- Permanente

- Par horaires
- Par jours de la semaine

Interdiction de tout accès réseau

Les groupes de machines

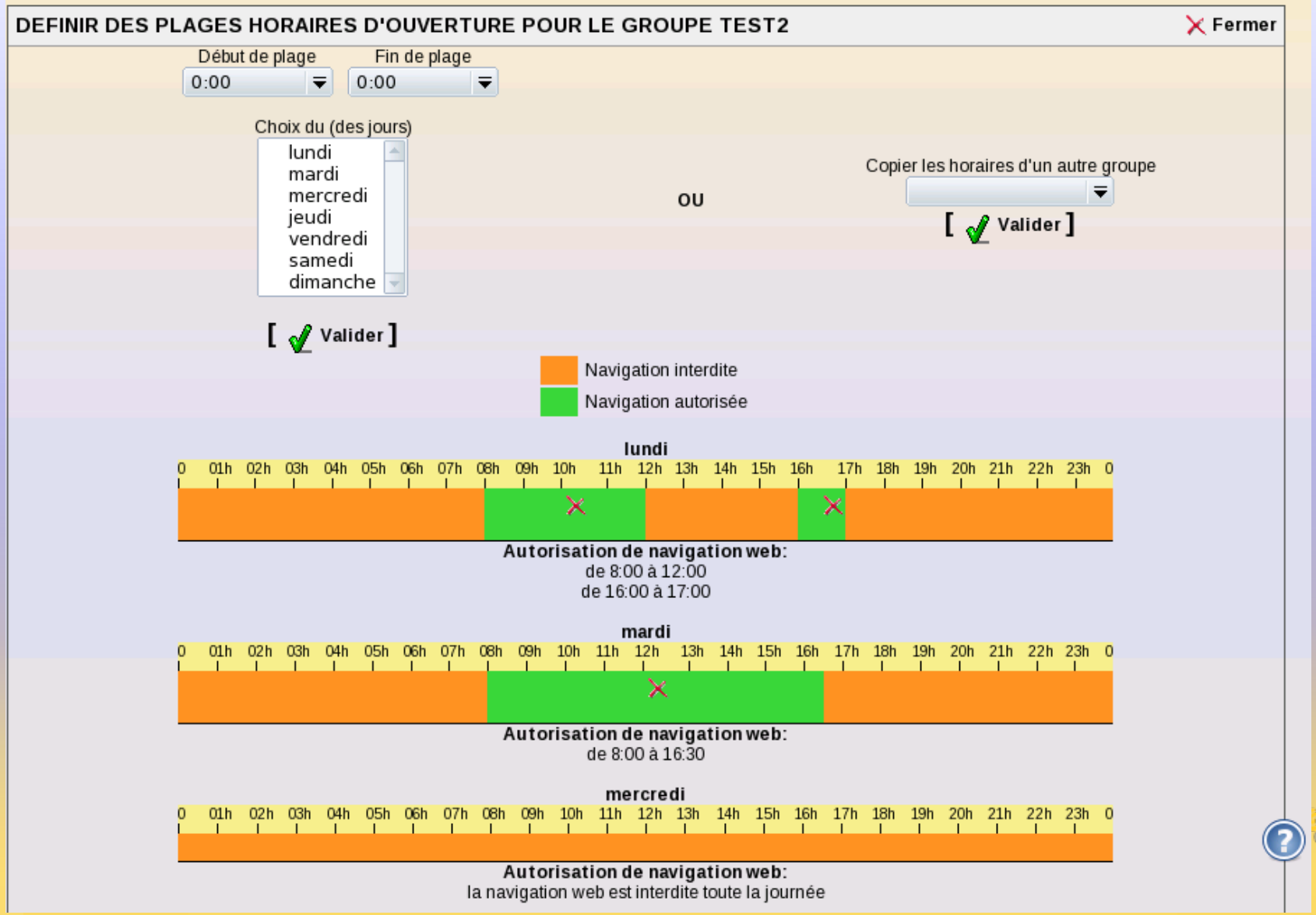
GROUPE DE MACHINE

[Nouveau groupe de machine]

LISTE DES GROUPES DE MACHINE

Groupes de machine	horaires	Interdictions	politique optionnelle	suppression
cdi plage IP: 172.17.0.31 à 172.17.0.40 sur l'interface eth2		Jamais	Défaut	
maternelle plage IP: 172.17.0.51 à 172.17.0.60 sur l'interface eth2		Jamais	liste blanche	
techno plage IP: 172.17.0.41 à 172.17.0.50 sur l'interface eth2		Jamais	Défaut	
test2 plage IP: 172.17.0.23 à 172.17.0.30 sur l'interface eth2		Toute activit	Défaut	

Les groupes de machines



L'antivirus Web

Scan temps-réel des fichiers téléchargés

Base anti-virus mise à jour automatiquement

L'antivirus Web

ACCES INTERDIT

Utilisateur : **admineole**
IP Machine : **10.121.11.44**

Adresse refusée :
http://www.eicar.org/download/eicar.com
Raison :
Virus or bad content detected. Eicar-Test-Signature

Toutes vos demandes sont enregistrées. Des filtres sont appliqués.

Vous avez fait une tentative d'accès à un site Web qui ne présente aucun intérêt pour des besoins d'information pédagogique ou technique correspondant à votre classe d'utilisation.

Pour toute réclamation, adressez un message à : cachemaster@ac-dijon.fr

Powered by DansGuardian

Les règles de pare-feu

Règles optionnelles Era

Définies au niveau académique

(Dés)activables localement

Les règles de pare-feu

DÉFINIR LES RÈGLES DU PARE-FEU SUR LA ZONE 2

Activez/Désactivez des règles optionnelles

	Actif	Inactif
Interdire l'utilisation des dialogues en direct	○	●
Interdiction des protocoles de messagerie	○	●
Interdiction des forums	○	●
Interdire les connexions FTP	○	●
Internet restreint	○	●

[✓ Valider]

Le filtrage de protocole

L7Filter

Détection du protocole par expressions régulières « *patterns* »

- Indépendant des ports source et destination

Utilise la couche « *Application* » du modèle OSI (International Standards Organisation)

Le filtrage de protocole

Intégré à « *netfilter* »

Gestion possible d'horaire

QOS

Merci de votre attention