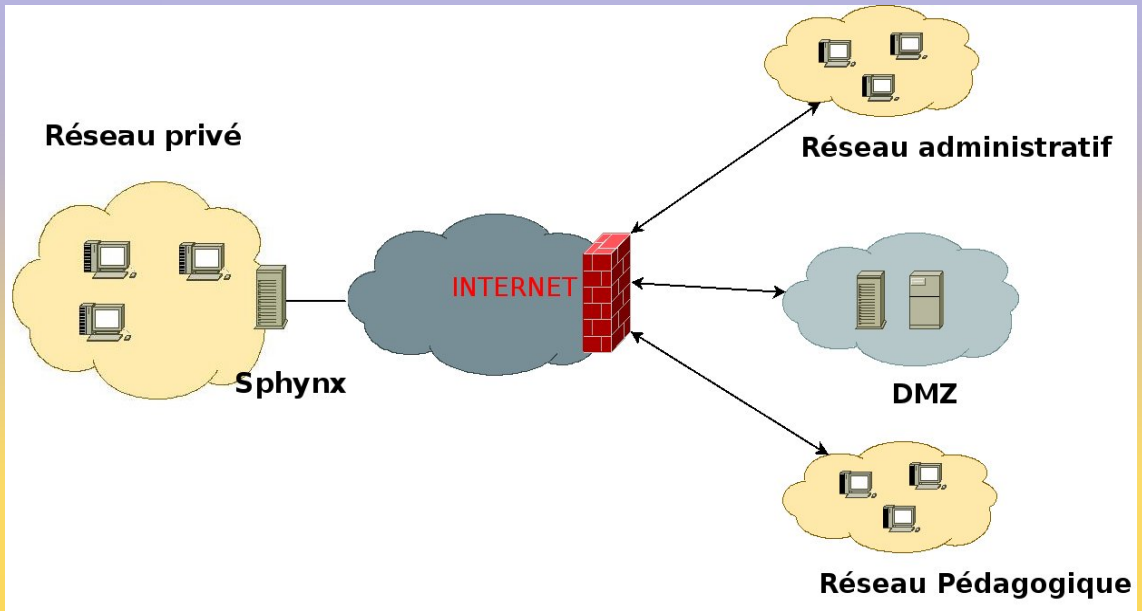
Séminaire EOLE
Dijon
23-24 Octobre 2008

AMON NG

Présentation

- Module Parefeu.
- Filtrage des accès réseaux (IP, Utilisateur)
- Filtrage et authentification des accès aux sites Internet
- Chiffrement du trafic réseau pour accéder à des réseaux privés distant (Sphynx).

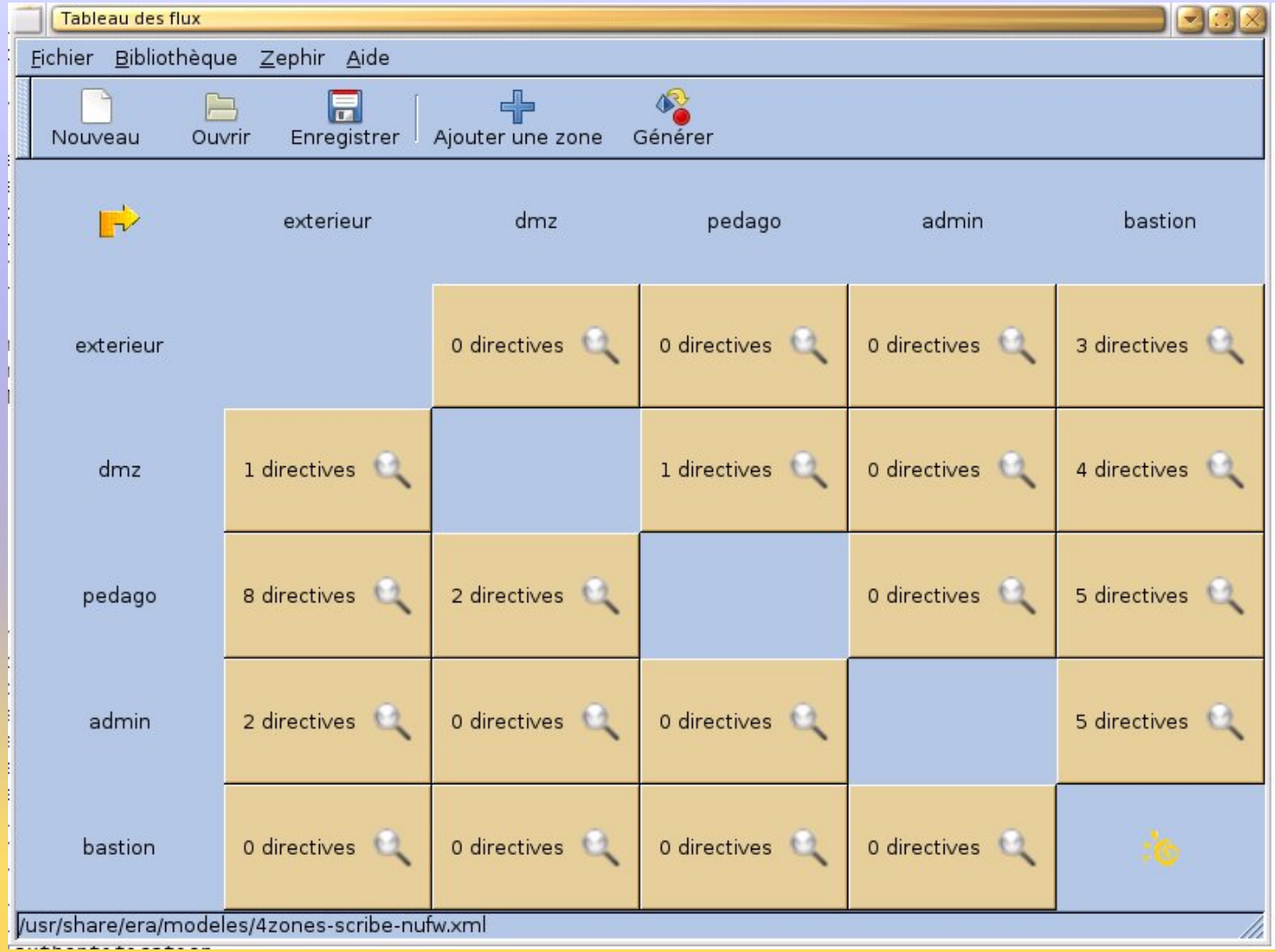


Présentation

- Interface de gestion : EAD

Présentation

- Interface de gestion de règles : Era



Nouveautés AmonNG (1)

- Authentification multi-NTLM.
- Ead multi-utilisateurs (SSO).
- Interdiction de sources/destinations via l'Ead.
- Mode de filtrage multi-configuration.
- Client bande passante Eole

Nouveautés AmonNG (1)

- Authentification des accès réseaux (NuFw)
- Journalisation (Log) centralisés
- Interfaçage de la gestion de la qualité de service (QOS)
- Amélioration SSO

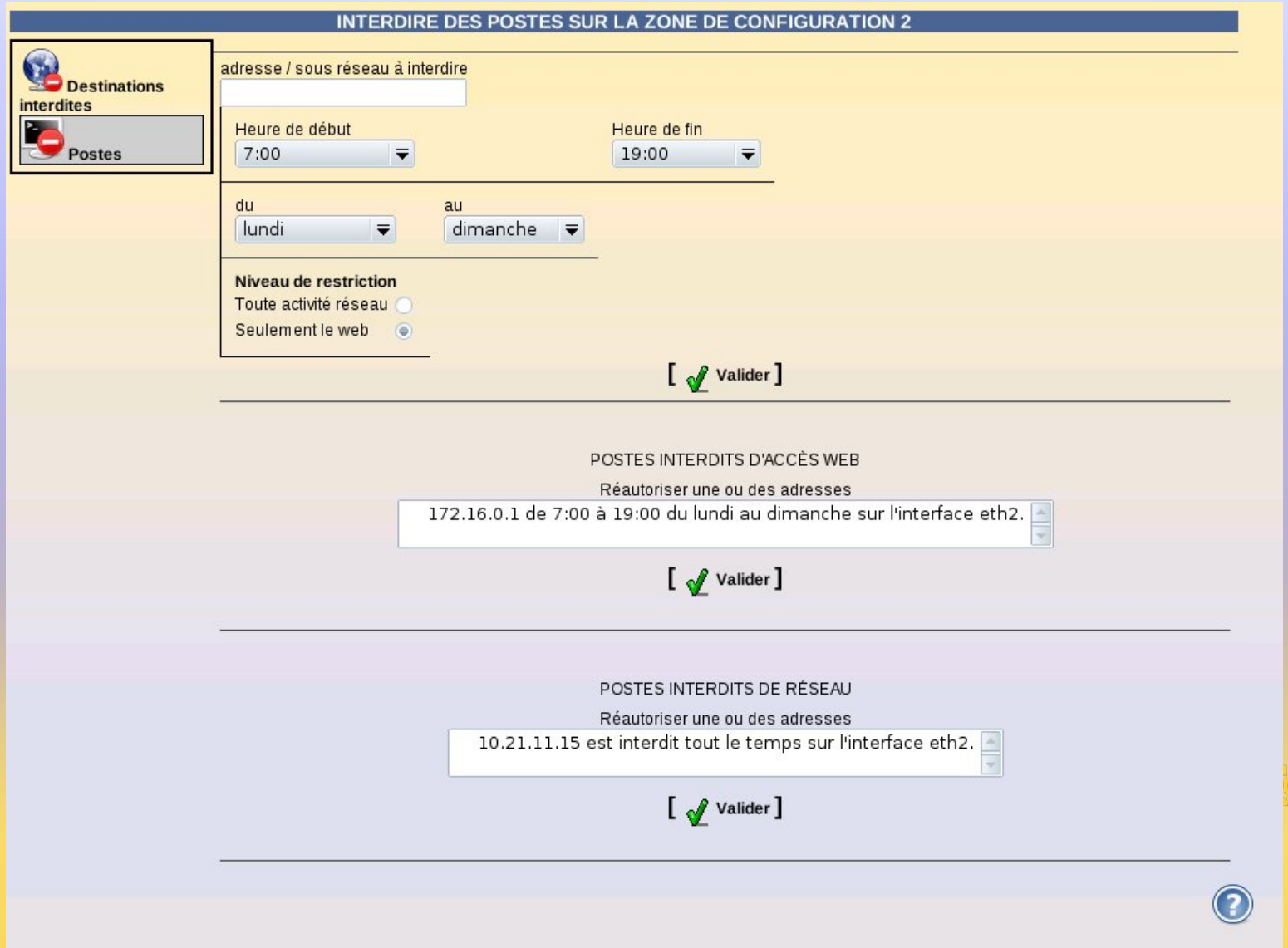
Authentification des accès aux sites

- LDAP
- NTLM (multi-domaine), authentification depuis un domaine Windows/Samba

Ead multi-utilisateur

- Authentification centralisée (SSO)
- Gestion de rôles

Interdiction de sources/destinations via l'Ead



LISTE DES GROUPES DE MACHINE

Groupes de machine	horaires	Interdiction de web	suppression
Cdi plage IP: 172.16.77.30 à 172.16.77.40 sur l'interface eth1		Jamais	

Fermer

CDI

DEFINIR DES PLAGES HORAIRES D'OUVERTURE

Début de plage 0:00 Fin de plage 0:00

Choix du (des jours)
- lundi
- mardi
- mercredi
- jeudi
- vendredi
- samedi
- dimanche

[Valider]

OU

Copier les horaires d'un autre groupe

[Valider]

Navigation interdite
Navigation autorisée

lundi

0 01h 02h 03h 04h 05h 06h 07h 08h 09h 10h 11h 12h 13h 14h 15h 16h 17h 18h 19h 20h 21h 22h 23h 0

Autorisation de navigation web:

mardi

0 01h 02h 03h 04h 05h 06h 07h 08h 09h 10h 11h 12h 13h 14h 15h 16h 17h 18h 19h 20h 21h 22h 23h 0

Autorisation de navigation web:

mercredi

0 01h 02h 03h 04h 05h 06h 07h 08h 09h 10h 11h 12h 13h 14h 15h 16h 17h 18h 19h 20h 21h 22h 23h 0

Autorisation de navigation web:

jeudi

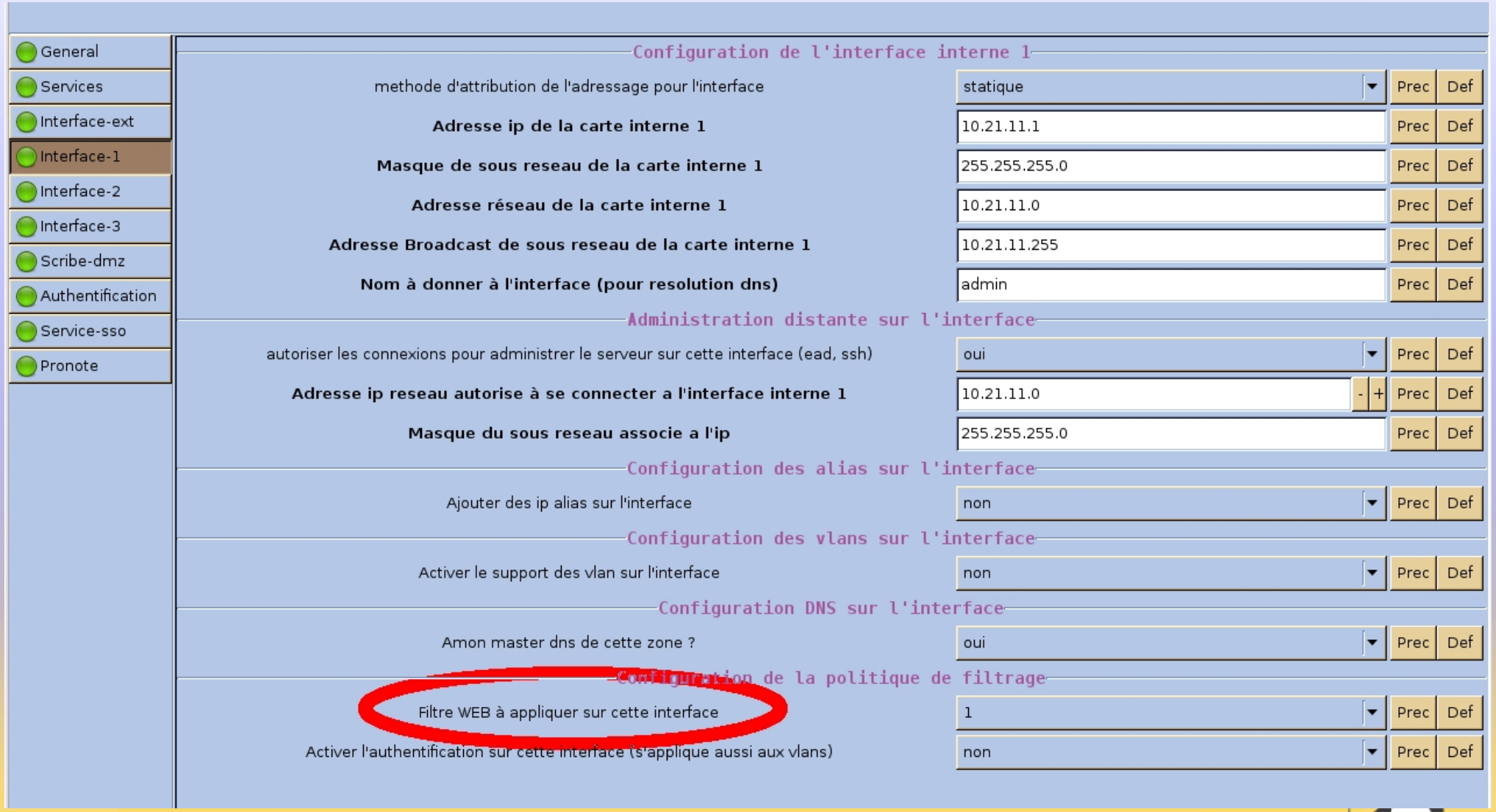
0 01h 02h 03h 04h 05h 06h 07h 08h 09h 10h 11h 12h 13h 14h 15h 16h 17h 18h 19h 20h 21h 22h 23h 0

Autorisation de navigation web:

Mode de filtrage multi-configuration

- Par zone
- Par politique

Les zones


General
Services
Interface-ext
Interface-1
Interface-2
Interface-3
Scribe-dmz
Authentification
Service-sso
Pronote
Configuration de l'interface interne 1
methode d'attribution de l'adressage pour l'interface
statique
Adresse ip de la carte interne 1
10.21.11.1
Masque de sous reseau de la carte interne 1
255.255.255.0
Adresse réseau de la carte interne 1
10.21.11.0
Adresse Broadcast de sous reseau de la carte interne 1
10.21.11.255
Nom à donner à l'interface (pour resolution dns)
admin
Administration distante sur l'interface
autoriser les connexions pour administrer le serveur sur cette interface (ead, ssh)
oui
Adresse ip reseau autorise à se connecter a l'interface interne 1
10.21.11.0
Masque du sous reseau associe a l'ip
255.255.255.0
Configuration des alias sur l'interface
Ajouter des ip alias sur l'interface
non
Configuration des vlans sur l'interface
Activer le support des vlan sur l'interface
non
Configuration DNS sur l'interface
Amon master dns de cette zone ?
oui
Configuration de la politique de filtrage
Filtre WEB à appliquer sur cette interface
1
Activer l'authentification sur cette interface (s'applique aussi aux vlans)
non
Prec
Def


Actions sur le serveur
Accueil
Configuration 1
Groupe de machine
Postes
Visites des sites
Sites
Règles du pare-feu
Utilisateurs
Configuration 2
Groupe de machine
Postes
Visites des sites
Sites
Règles du pare-feu
Configuration générale
Outils
Système
Édition de rôles

Les Politiques

- Par défaut
- Modérateur
- Interdit
- Liste blanche
- 3 configurations personnalisables

GESTION DES UTILISATEURS SUR LA ZONE DE CONFIGURATION 1

Login de l'utilsateur à gérer sur la zone de configuration 1

[Valider]

Modérateurs | Utilisateurs interdits | Utilisateurs en mode liste blanche

Login des utilisateurs	politique de filtrage	suppression
gaspard.alizan	interdits	✕
gerard.menvussa	modérateur	✕
leo.coudert	liste blanche	✕
zoe.dupont	3	✕

ACTIVATION DES FILTRES FACULTATIFS SUR LA ZONE DE CONFIGURATION 1

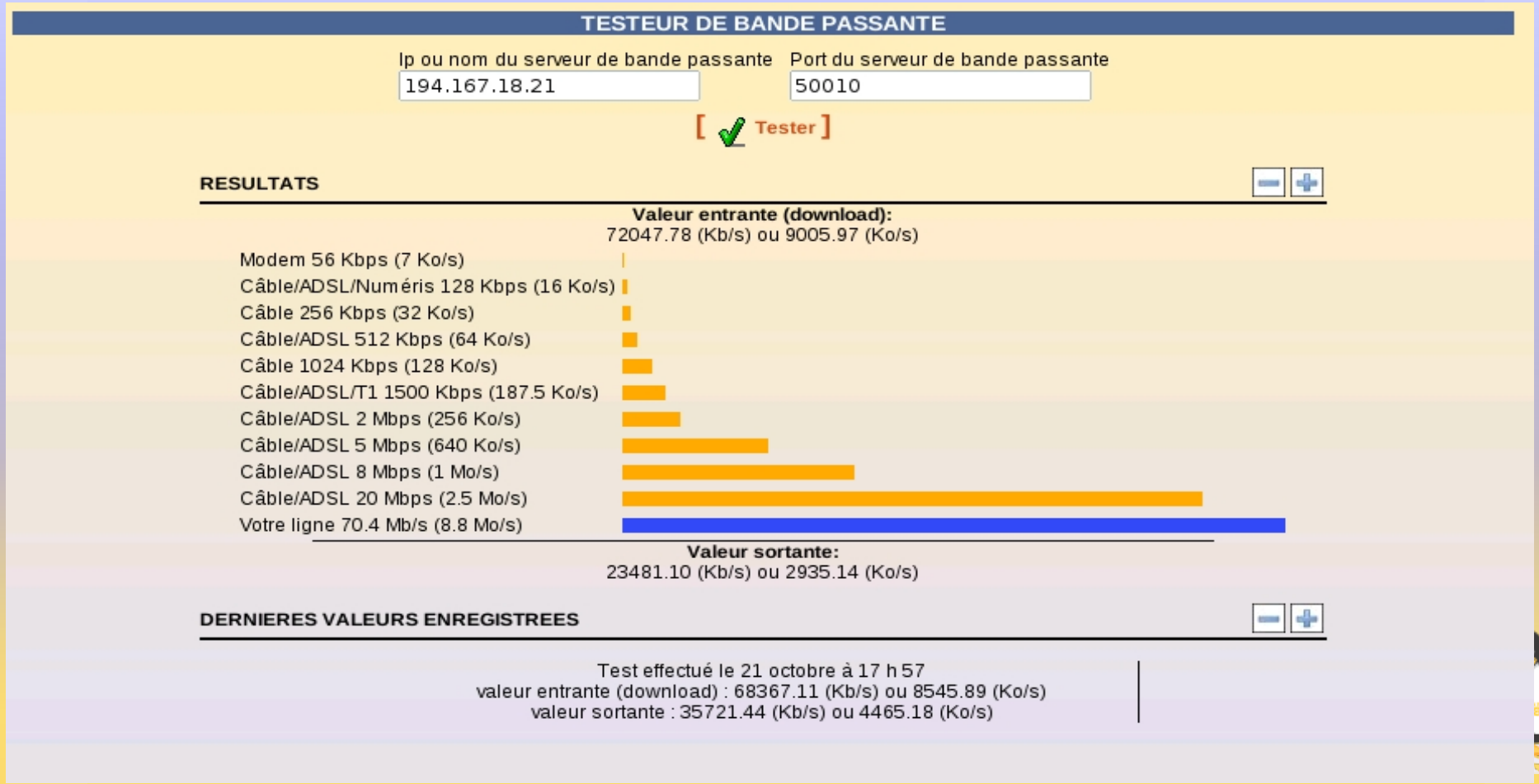
- Filtres
- Filtrage
- Sites interdits
- Sites autorisés
- Extensions
- Type MIME
- Sites du mode liste blanche

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]

Client bande passante Eole

- Permet de repérer les « goulots d'étranglement »



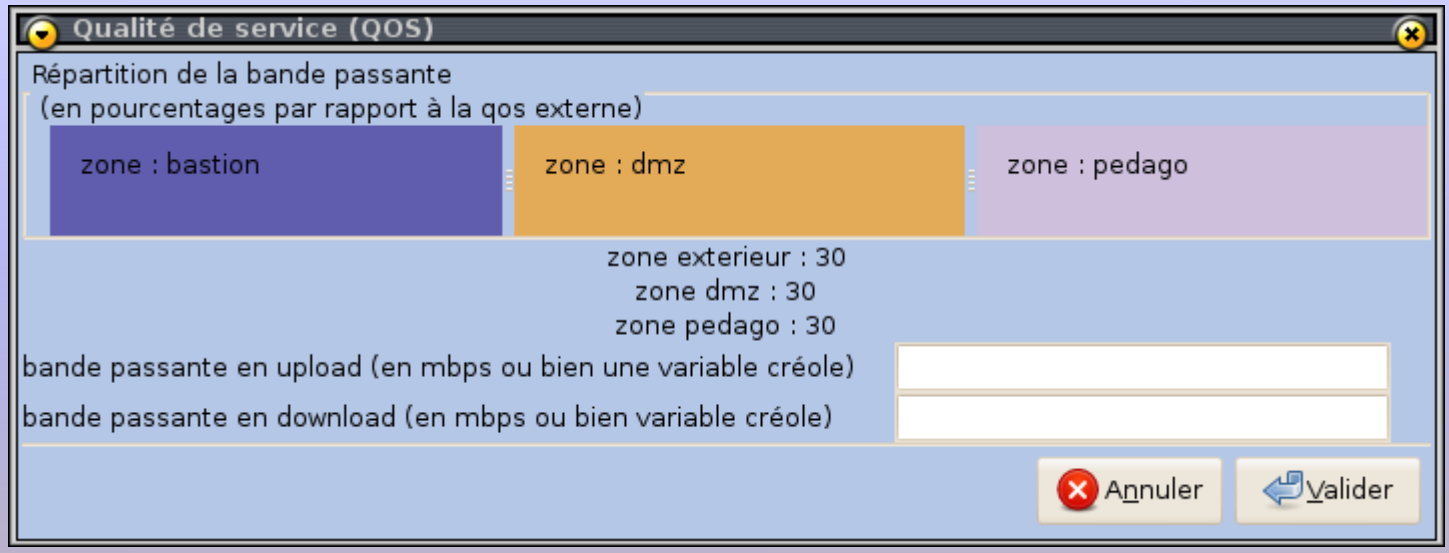
Authentification des accès réseaux (NuFw)

- Gestion des accès réseau en fonction de l'utilisateur
- Client NuFw intégré au client Scribe

Journalisation (Log) centralisés

- ZephirLog : centralisation des fichiers de log (accès squid, autres)
- Chiffrement des transferts
- Reprise en cas de coupure réseau

Interfaçage de la gestion de la qualité de service (QOS)



Merci de votre attention