



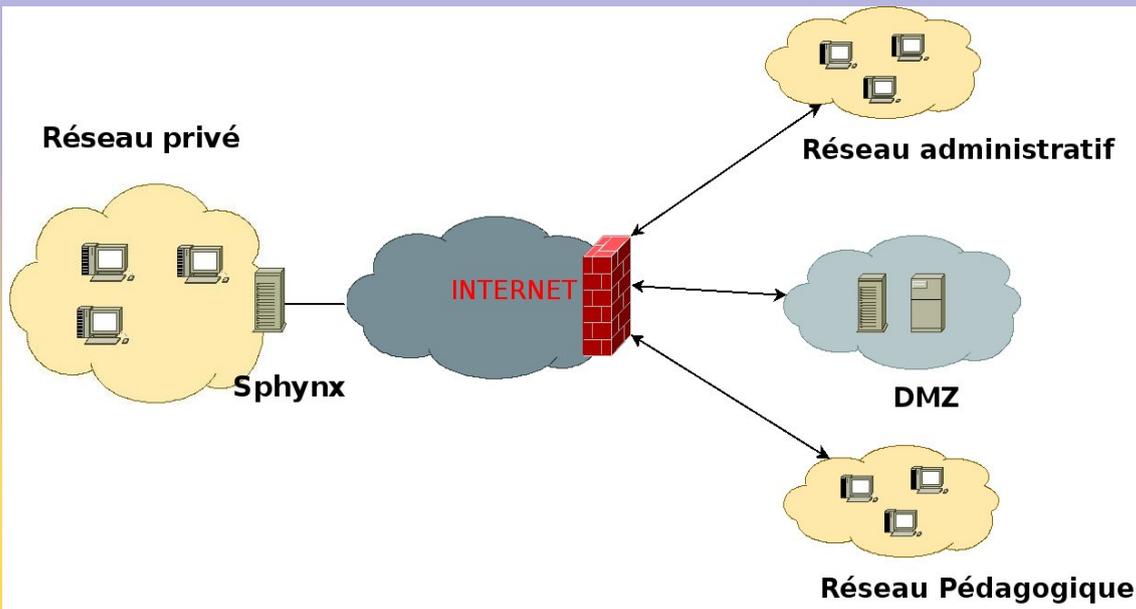
Séminaire EOLE
Dijon
23-24 Octobre 2008

AMON NG



Eole 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).



Eole Présentation

- Interface de gestion : EAD

Administration

Administration

pf-amon

VOUS ÊTES CONNECTÉ(E) EN TANT QUE ADMIN [Déconnexion](#)

MISE À JOUR

Dernière mise à jour :

COMPTE RENDU DE MISE À JOUR - MARDI 21 OCTOBRE 2008, 16:27:55 (UTC+0200)

[+ Afficher le rapport](#)

LISTE DE SITES INTERDITS

Dernière mise à jour :

Mise à jour le 10/22/08 :

[+ Afficher le rapport](#)

SERVICES

ETAT DES SERVICES

Services	DETAILS
Utilisation	DETAILS
Système	DETAILS

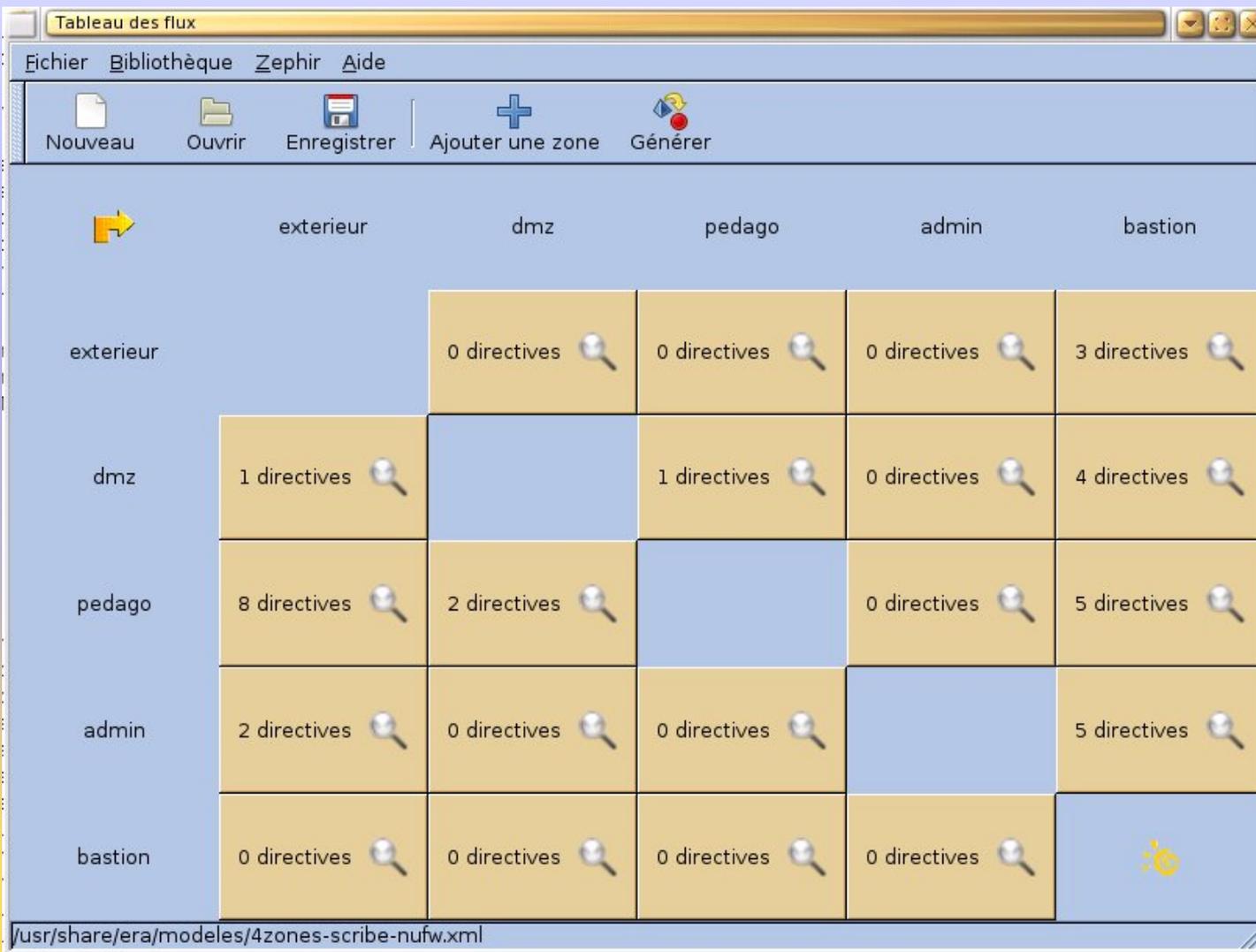
Actions sur le serveur

- Accueil
- Configuration 1
- Configuration 2
- Configuration générale
- Outils
- Système
- Édition de rôles



Eole Présentation

- Interface de gestion de règles : Era



The screenshot shows the 'Tableau des flux' (Traffic Table) interface in the Era tool. The interface includes a menu bar with 'Fichier', 'Bibliothèque', 'Zephir', and 'Aide'. Below the menu is a toolbar with icons for 'Nouveau', 'Ouvrir', 'Enregistrer', 'Ajouter une zone', and 'Générer'. The main area displays a traffic table with five zones: 'exterieur', 'dmz', 'pedago', 'admin', and 'bastion'. The table shows the number of rules for each zone-to-zone connection. The 'bastion' zone is highlighted with a yellow sun icon.

	exterieur	dmz	pedago	admin	bastion
exterieur		0 directives	0 directives	0 directives	3 directives
dmz	1 directives		1 directives	0 directives	4 directives
pedago	8 directives	2 directives		0 directives	5 directives
admin	2 directives	0 directives	0 directives		5 directives
bastion	0 directives	0 directives	0 directives	0 directives	

The status bar at the bottom shows the file path: /usr/share/era/modeles/4zones-scribe-nufw.xml



Eole 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



Le 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

INTERDIRE DES POSTES SUR LA ZONE DE CONFIGURATION 2

Destinations interdites

Postes

adresse / sous réseau à interdire

Heure de début: 7:00
Heure de fin: 19:00

du: lundi
au: dimanche

Niveau de restriction

Toute activité réseau

Seulement le web

[✓ Valider]

POSTES INTERDITS D'ACCÈS WEB

Réautoriser une ou des adresses

172.16.0.1 de 7:00 à 19:00 du lundi au dimanche sur l'interface eth2.

[✓ Valider]

POSTES INTERDITS DE RÉSEAU

Réautoriser une ou des adresses

10.21.11.15 est interdit tout le temps sur l'interface eth2.

[✓ Valider]





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

ou

Copier les horaires d'un autre groupe

▼

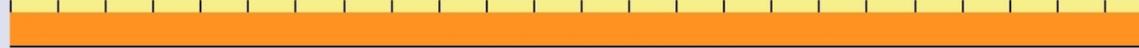
[✓ Valider]

[✓ 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

<ul style="list-style-type: none"> <input type="radio"/> General <input type="radio"/> Services <input type="radio"/> Interface-ext <input checked="" type="radio"/> Interface-1 <input type="radio"/> Interface-2 <input type="radio"/> Interface-3 <input type="radio"/> Scribe-dmz <input type="radio"/> Authentification <input type="radio"/> Service-sso <input type="radio"/> Pronote 	<p style="text-align: center;">Configuration de l'interface interne 1</p> <p>methode d'attribution de l'adressage pour l'interface: <input type="text" value="statique"/> <input type="button" value="Prec"/> <input type="button" value="Def"/></p> <p>Adresse ip de la carte interne 1: <input type="text" value="10.21.11.1"/> <input type="button" value="Prec"/> <input type="button" value="Def"/></p> <p>Masque de sous reseau de la carte interne 1: <input type="text" value="255.255.255.0"/> <input type="button" value="Prec"/> <input type="button" value="Def"/></p> <p>Adresse réseau de la carte interne 1: <input type="text" value="10.21.11.0"/> <input type="button" value="Prec"/> <input type="button" value="Def"/></p> <p>Adresse Broadcast de sous reseau de la carte interne 1: <input type="text" value="10.21.11.255"/> <input type="button" value="Prec"/> <input type="button" value="Def"/></p> <p>Nom à donner à l'interface (pour resolution dns): <input type="text" value="admin"/> <input type="button" value="Prec"/> <input type="button" value="Def"/></p> <p style="text-align: center;">Administration distante sur l'interface</p> <p>autoriser les connexions pour administrer le serveur sur cette interface (ead, ssh): <input type="text" value="oui"/> <input type="button" value="Prec"/> <input type="button" value="Def"/></p> <p>Adresse ip reseau autorise à se connecter a l'interface interne 1: <input type="text" value="10.21.11.0"/> <input type="button" value="-"/> <input type="button" value="+"/> <input type="button" value="Prec"/> <input type="button" value="Def"/></p> <p>Masque du sous reseau associe a l'ip: <input type="text" value="255.255.255.0"/> <input type="button" value="Prec"/> <input type="button" value="Def"/></p> <p style="text-align: center;">Configuration des alias sur l'interface</p> <p>Ajouter des ip alias sur l'interface: <input type="text" value="non"/> <input type="button" value="Prec"/> <input type="button" value="Def"/></p> <p style="text-align: center;">Configuration des vlans sur l'interface</p> <p>Activer le support des vlan sur l'interface: <input type="text" value="non"/> <input type="button" value="Prec"/> <input type="button" value="Def"/></p> <p style="text-align: center;">Configuration DNS sur l'interface</p> <p>Amon master dns de cette zone?: <input type="text" value="oui"/> <input type="button" value="Prec"/> <input type="button" value="Def"/></p> <p style="text-align: center;">Configuration de la politique de filtrage</p> <p>Filtre WEB à appliquer sur cette interface: <input type="text" value="1"/> <input type="button" value="Prec"/> <input type="button" value="Def"/></p> <p>Activer l'authentification sur cette interface (s'applique aussi aux vlans): <input type="text" value="non"/> <input type="button" value="Prec"/> <input type="button" value="Def"/></p>
--	---



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'utilisateur 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
	<u>tous</u> <u>aucun</u>	<u>tous</u> <u>aucun</u>	<u>tous</u> <u>aucun</u>	<u>tous</u> <u>aucun</u>
contenus agressifs (xenophobie...)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
audio/video	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
téléphones mobiles, sonneries	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
radios en ligne	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
drogue	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
mail et chat	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
webmail les plus connus	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
jeux de hasard et d'argent	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
jeux en ligne	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
hacking (piratage)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
phishing	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
warez (piratage)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
triche aux examens	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
bandeaux publicitaires	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
divers (humour...)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
utilisation de proxy distants	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
proxy spécifiques	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

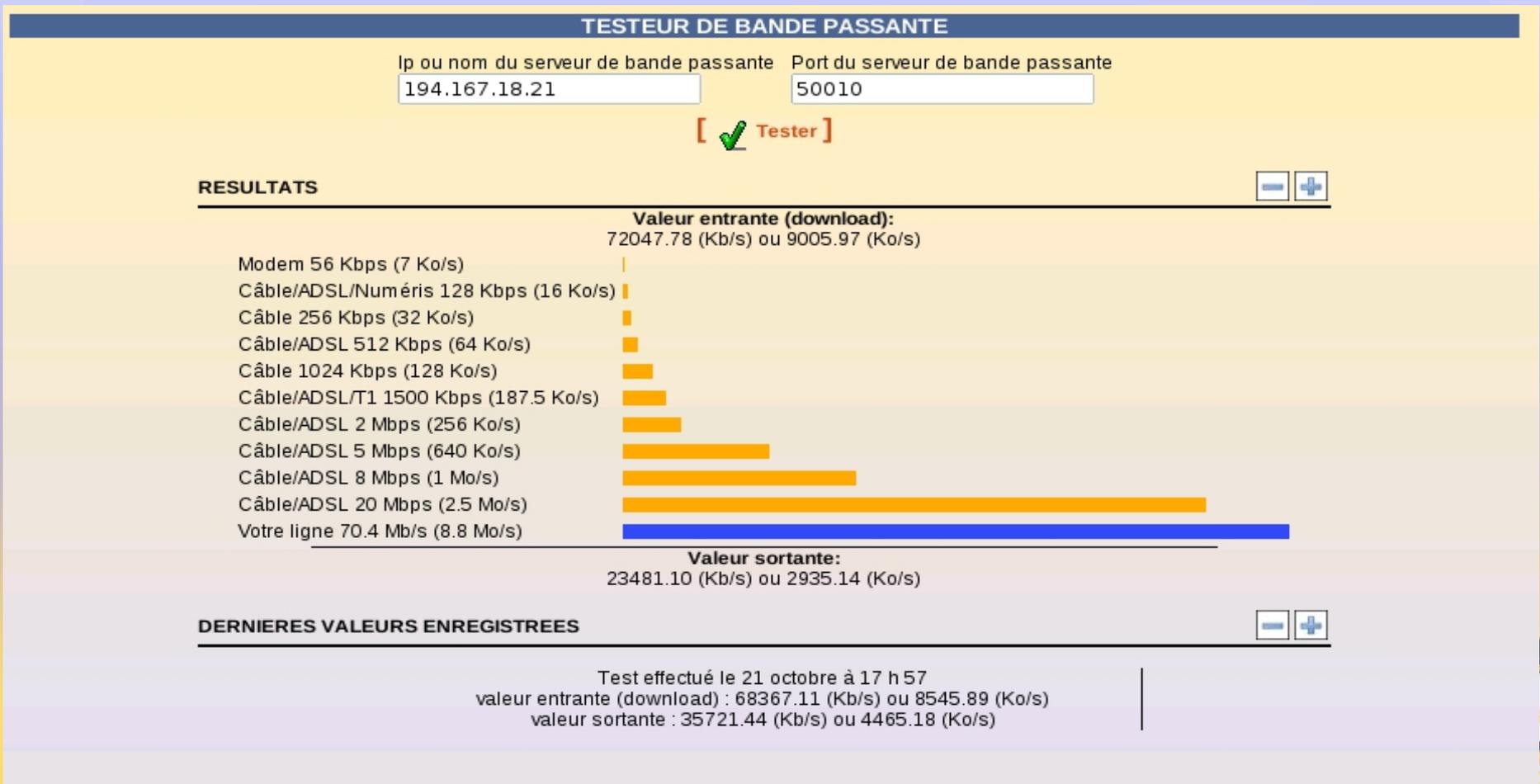
[ Valider]





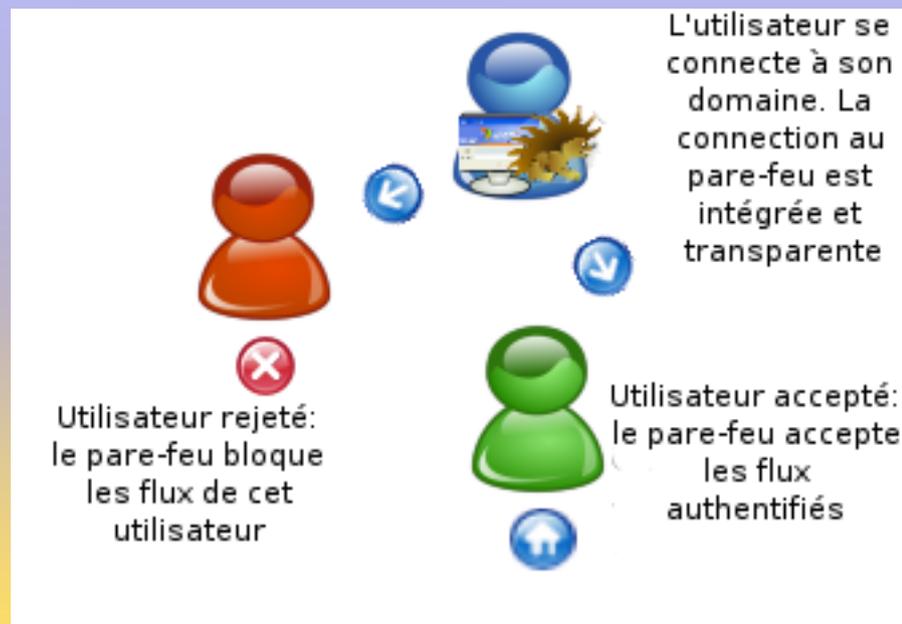
Client bande passante Eole

- 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)

Qualité de service (QOS)

Répartition de la bande passante
(en pourcentages par rapport à la qos externe)

zone : bastion	zone : dmz	zone : pedago
----------------	------------	---------------

zone exterieur : 30
zone dmz : 30
zone pedago : 30

bande passante en upload (en mbps ou bien une variable créole)

bande passante en download (en mbps ou bien variable créole)





Merci de votre attention

