Séminaire EOLE
DIJON
20 et 21 Octobre 2009

Amon NG, fonctionnalités réseaux

Introduction

Vlans

Agrégation de liens

QOS

Radius

Filtrage réseau authentifié

NTLM - Kerberos

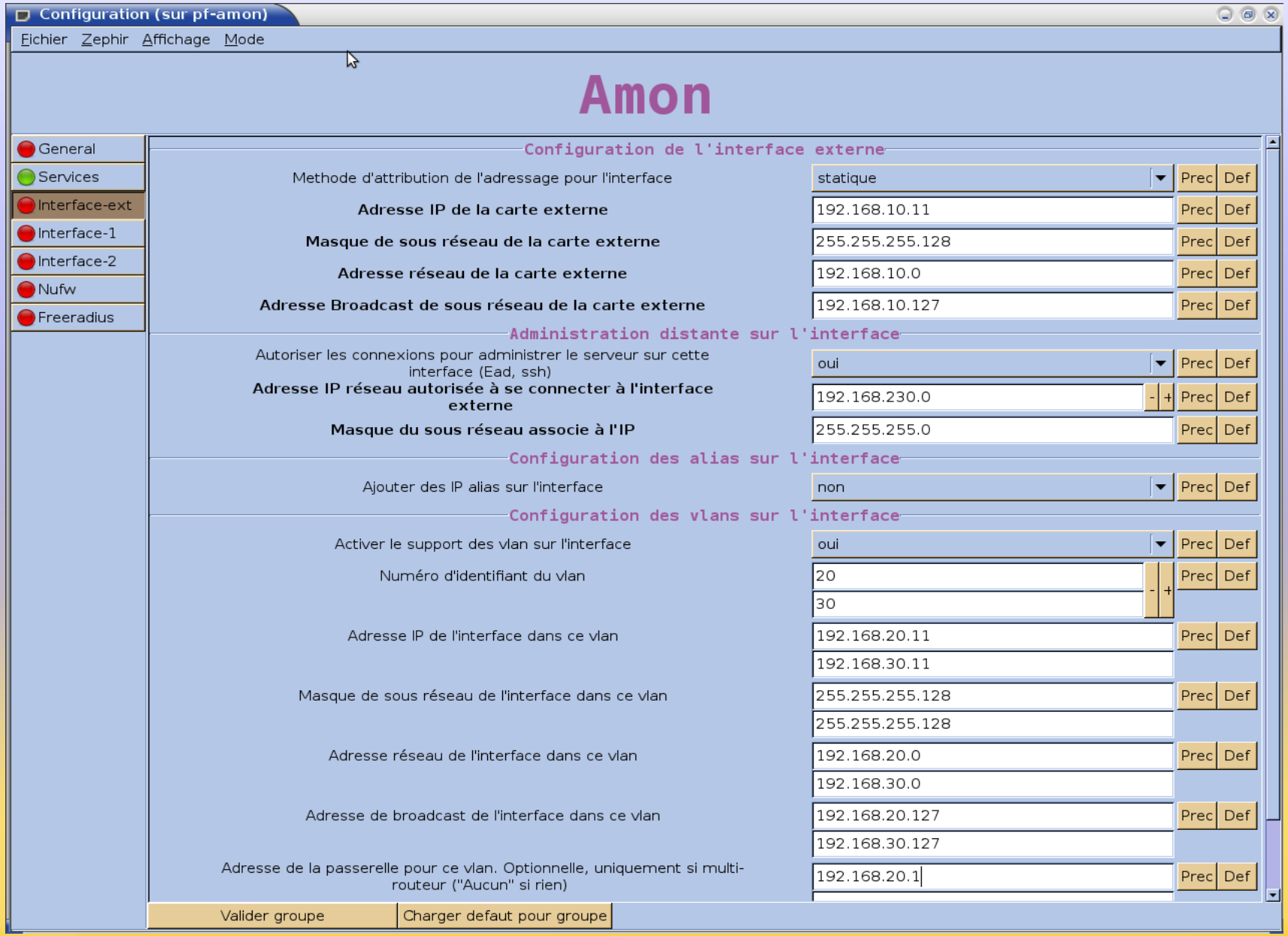
Vlans (1)

Amon est capable de gérer le protocole 802.1q (Vlans).

Possibilité d'affecter plusieurs Vlans pour chacune des interfaces physiques.

- L'interface physique est considérée comme étant un Vlan 'natif'.
- Au niveau proxy, les acls des Vlans sont les mêmes que les acls de l'interface.
- Idem pour le DNS.
- Toute la partie filtrage IP au niveau d'Era n'est pas automatique.

Vlans (2)


Configuration (sur pf-amon)
Fichier Zephir Affichage Mode
Amon
General
Services
Interface-ext
Interface-1
Interface-2
Nufw
Freeradius
Configuration de l'interface externe
Methode d'attribution de l'adressage pour l'interface
statique
Adresse IP de la carte externe
192.168.10.11
Masque de sous réseau de la carte externe
255.255.255.128
Adresse réseau de la carte externe
192.168.10.0
Adresse Broadcast de sous réseau de la carte externe
192.168.10.127
Administration distante sur l'interface
Autoriser les connexions pour administrer le serveur sur cette interface (Ead, ssh)
oui
Adresse IP réseau autorisée à se connecter à l'interface externe
192.168.230.0
Masque du sous réseau associe à 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
oui
Numéro d'identifiant du vlan
20
30
Adresse IP de l'interface dans ce vlan
192.168.20.11
192.168.30.11
Masque de sous réseau de l'interface dans ce vlan
255.255.255.128
255.255.255.128
Adresse réseau de l'interface dans ce vlan
192.168.20.0
192.168.30.0
Adresse de broadcast de l'interface dans ce vlan
192.168.20.127
192.168.30.127
Adresse de la passerelle pour ce vlan. Optionnelle, uniquement si multi-routeur ("Aucun" si rien)
192.168.20.1
Prec
Def
Valider groupe
Charger defaut pour groupe

Vlans (3)

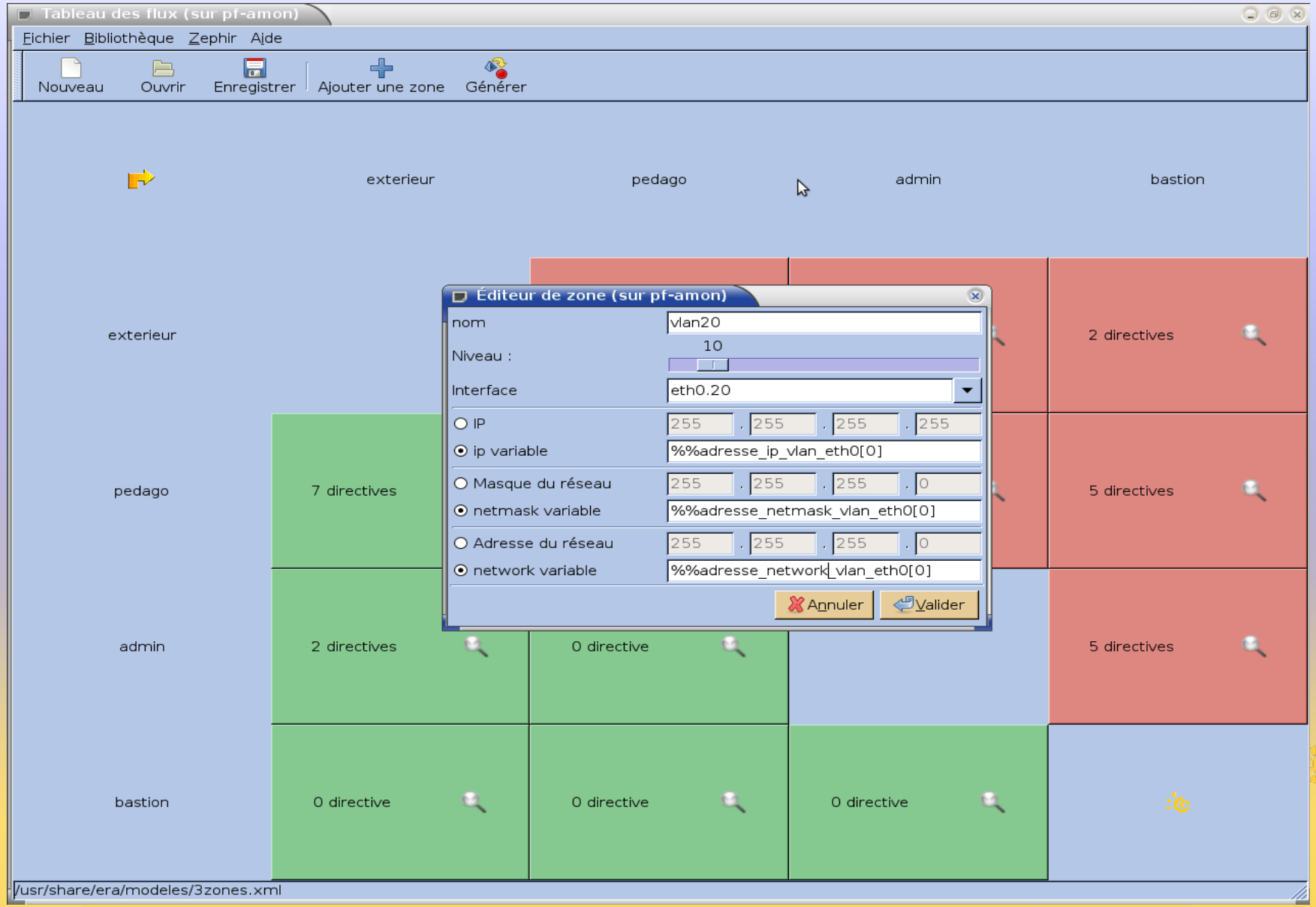


Tableau des flux (sur pf-amon)
Fichier Bibliothèque Zephir Aide
Nouveau
Ouvrir
Enregistrer
Ajouter une zone
Générer
exterieur
pedago
admin
bastion
2 directives
7 directives
5 directives
2 directives
0 directive
5 directives
0 directive
0 directive
0 directive
Éditeur de zone (sur pf-amon)
nom
vlan20
Niveau :
10
Interface
eth0.20
IP
255 . 255 . 255 . 255
ip variable
%%adresse_ip_vlan_eth0[0]
Masque du réseau
255 . 255 . 255 . 0
netmask variable
%%adresse_netmask_vlan_eth0[0]
Adresse du réseau
255 . 255 . 255 . 0
network variable
%%adresse_network_vlan_eth0[0]
Annuler
Valider
/usr/share/era/modeles/3zones.xml

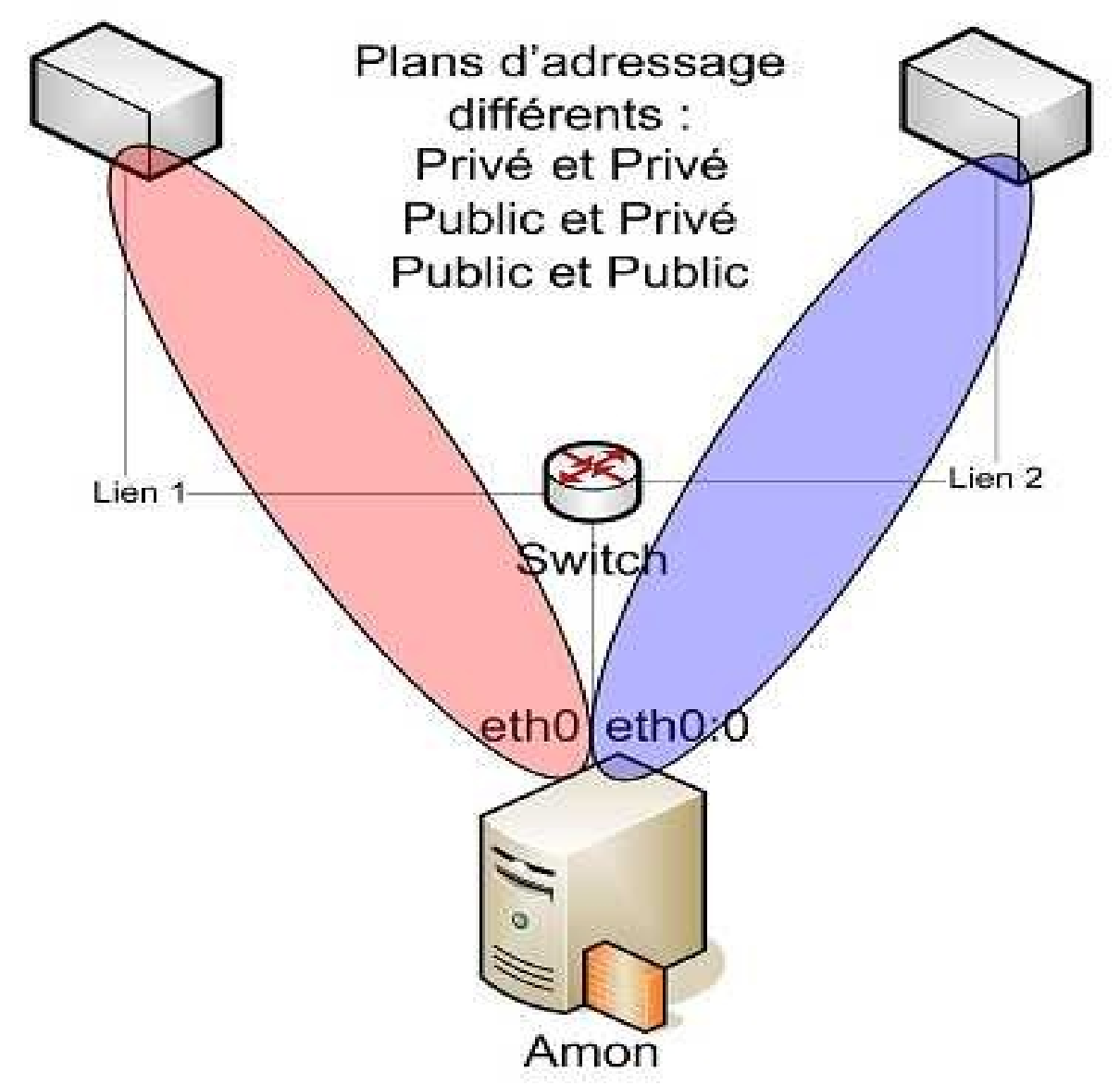
Agrégation de Liens (1)

Intégration de travaux effectués par les académies de Versailles, de Nantes et de Créteil.

Permet d'utiliser 2 abonnements Internet afin de garantir une meilleur qualité de service.

Repose sur un principe simple de pondération des routes avec un mécanisme de bascule en cas de dysfonctionnement d'un des liens.

Agrégation de Liens (2)



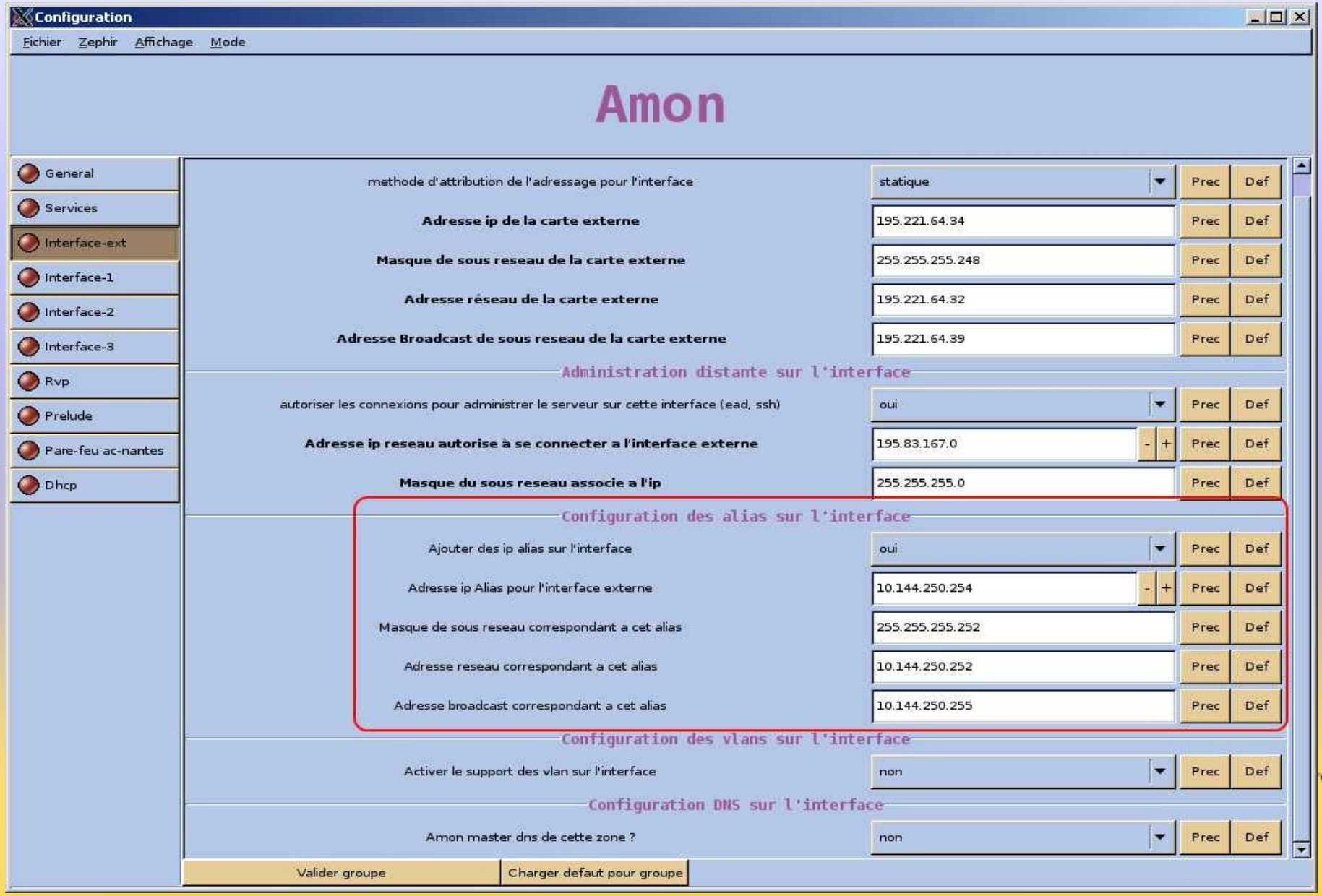
Agrégation de Liens (3)

Un service surveille l'état des liens en effectuant des requêtes régulières sur chacun d'eux.

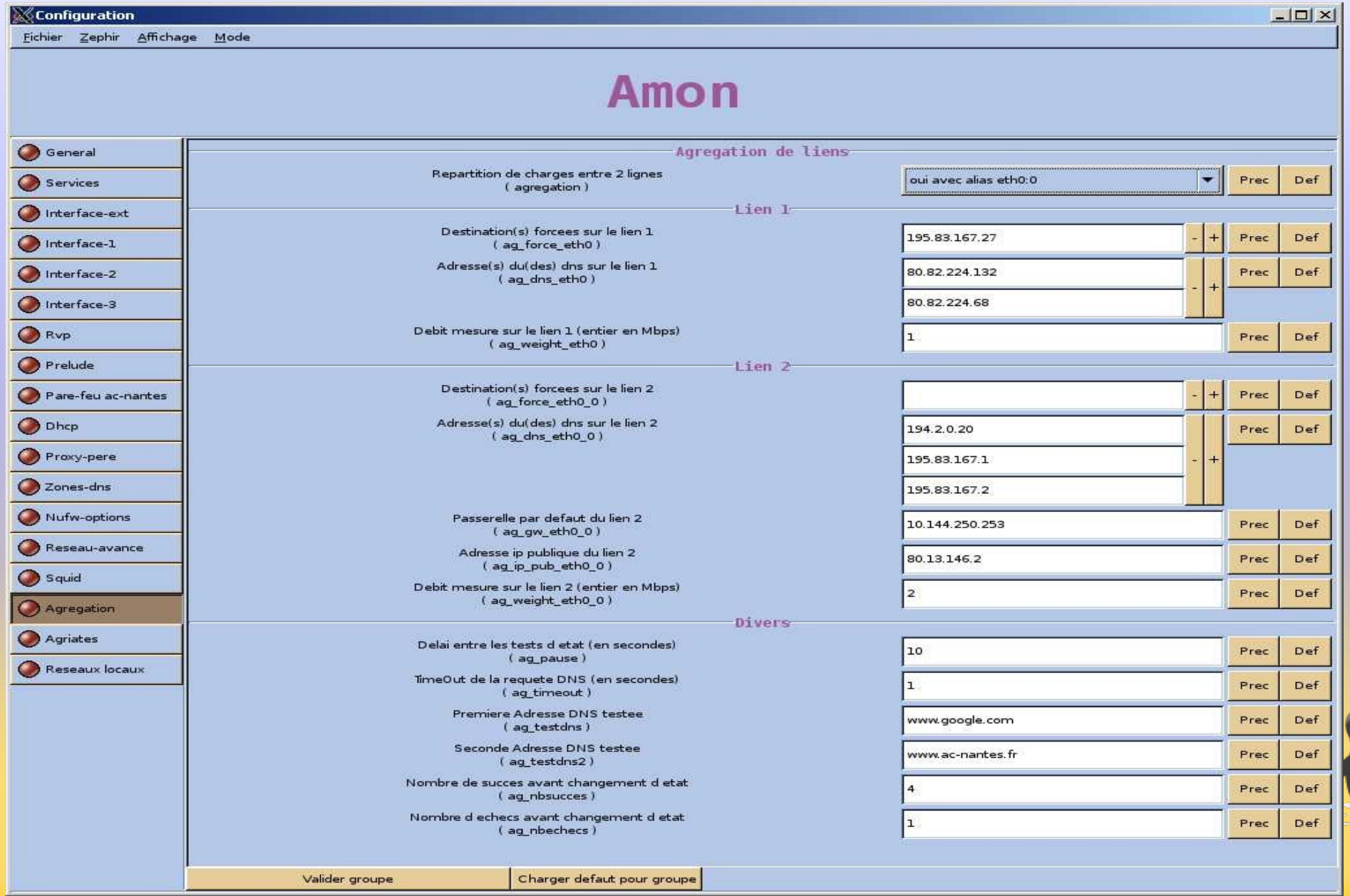
Lors d'un changement d'état

- Si le lien 1 est tombé, tout le trafic est redirigé vers le lien 2
- Si le lien 2 est tombé, tout le trafic est redirigé vers le lien 1
- La configuration est remise à son état initiale au retour de l'un ou l'autre des liens.

Agrégation de Liens (4)



Agrégation de Liens (5)



Agrégation de Liens (6)

Exemple de logs du service

```
Le lien 2 est tombe
Le lien 2 est tombe
L'etat du lien 2 a change de 1 a 0
L'etat du lien 2 va changer de 1
Rechargement de la repartition sur les 2 liens
Erreur de resolution de www.google.com sur le dns 194.2.0.20 du lien 2
Erreur de resolution de www.google.com sur le dns 195.83.167.1 du lien 2
Erreur de resolution de www.google.com sur le dns 195.83.167.2 du lien 2
Erreur de resolution de www.ac-nantes.fr sur le dns 194.2.0.20 du lien 2
Erreur de resolution de www.ac-nantes.fr sur le dns 195.83.167.1 du lien 2
Erreur de resolution de www.ac-nantes.fr sur le dns 195.83.167.2 du lien 2
Le lien 2 est tombe
L'etat du lien 2 a change de 0 a 1
L'etat du lien 2 va changer de 0
Passage sur le lien 1
L'etat du lien 2 a change de 1 a 0
L'etat du lien 2 va changer de 1
Rechargement de la repartition sur les 2 liens
Erreur de resolution de www.google.com sur le dns 80.82.224.132 du lien 1
Erreur de resolution de www.google.com sur le dns 80.82.224.68 du lien 1
Erreur de resolution de www.ac-nantes.fr sur le dns 80.82.224.132 du lien 1
Erreur de resolution de www.ac-nantes.fr sur le dns 80.82.224.68 du lien 1
Le lien 1 est tombe
L'etat du lien 1 a change de 0 a 1
L'etat du lien 1 va changer de 0
Erreur de resolution de www.google.com sur le dns 194.2.0.20 du lien 2
Passage sur le lien 2
```

QOS (1)

Il s'agit plus d'un mécanisme de partage de la bande passante que de de la Qos à proprement parlé (type DiffServ)

Permet de garantir une bande passante minimale par rapport à l'extérieur

La gestion de la Qos se fait depuis Era.

QOS (2)


repartition de la bande passante (en pourcentages)
zone : bastion
zone : pedago
zone : admin
zone exterieur : 17
zone pedago : 55
zone admin : 18
bande passante en upload
%%upload_bandwidth
bande passante en download
%%download_bandwidth
Annuler
Valider

QOS (3)


Options du modèle (sur pf-amon)
option
option activée
qos
netbios
Annuler
Valider

Radius (1)

Intégration de freeradius (version 2.1.7) au niveau d'Amon.

Radius : Remote Access Dial In User Service

- Protocole d'authentification réseau.
- Offre une sécurité avancée pour des systèmes de points d’accès au réseau.

Deux sortes d'authentification RADIUS :

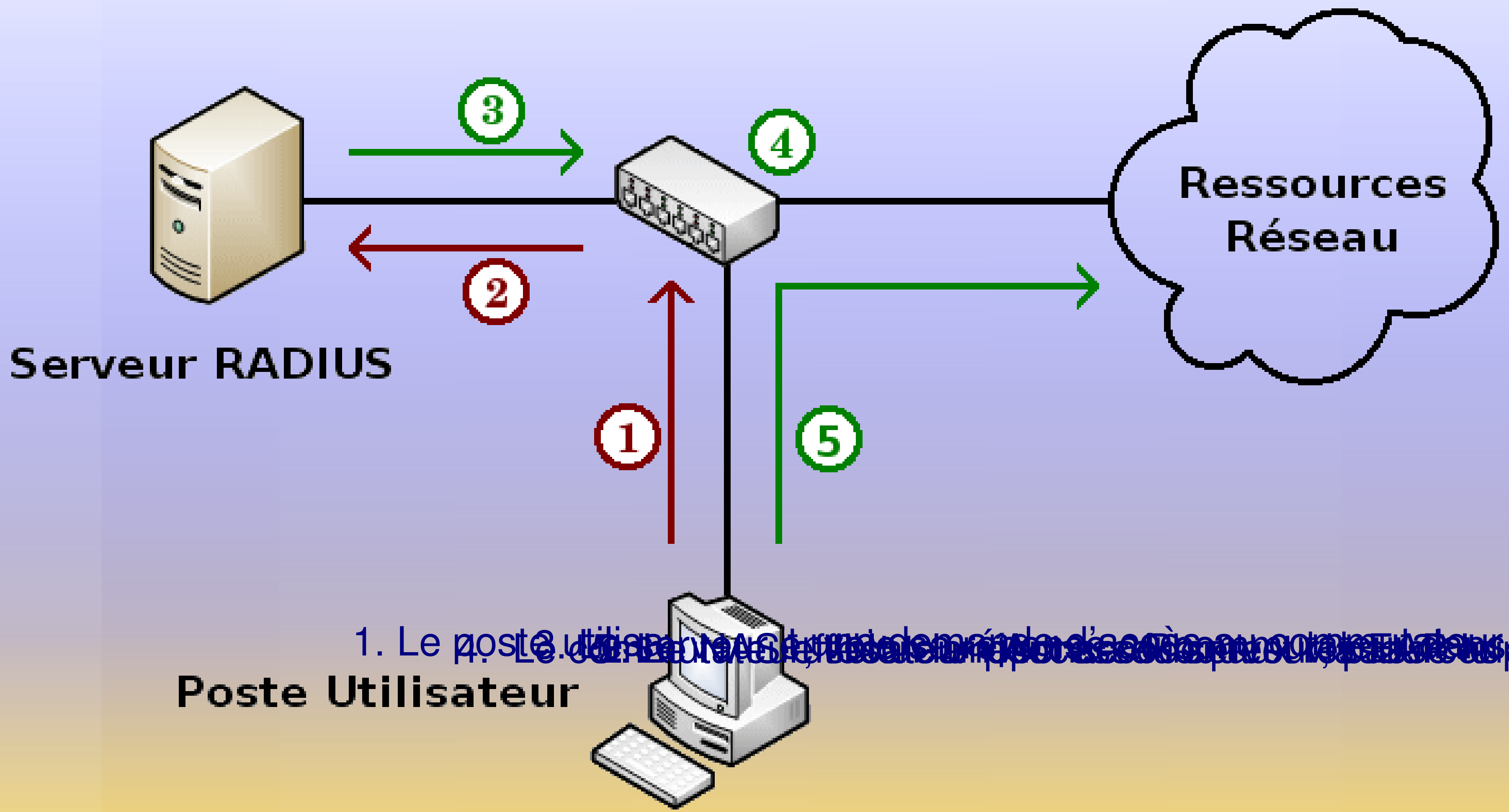
- Basée sur l'adresse MAC de la carte Ethernet.
- Basée sur le protocole 802.1x.

Radius (2)

Utilité 802.1X :

- Sécuriser les réseaux.
  - Assure une validation de l'accès au médium.
  - Limite en amont les intrusions sur le réseau.
  - Enregistre éventuellement les opérations de chaque utilisateur.
- Faciliter la gestion pour les administrateurs.
- Permettre la mobilité des utilisateurs.
  - Banalisation des postes.
  - Intégration des postes nomades (portables, etc.)
  - Prise en compte des connexions sans fils.

Radius (3)



Radius (4)

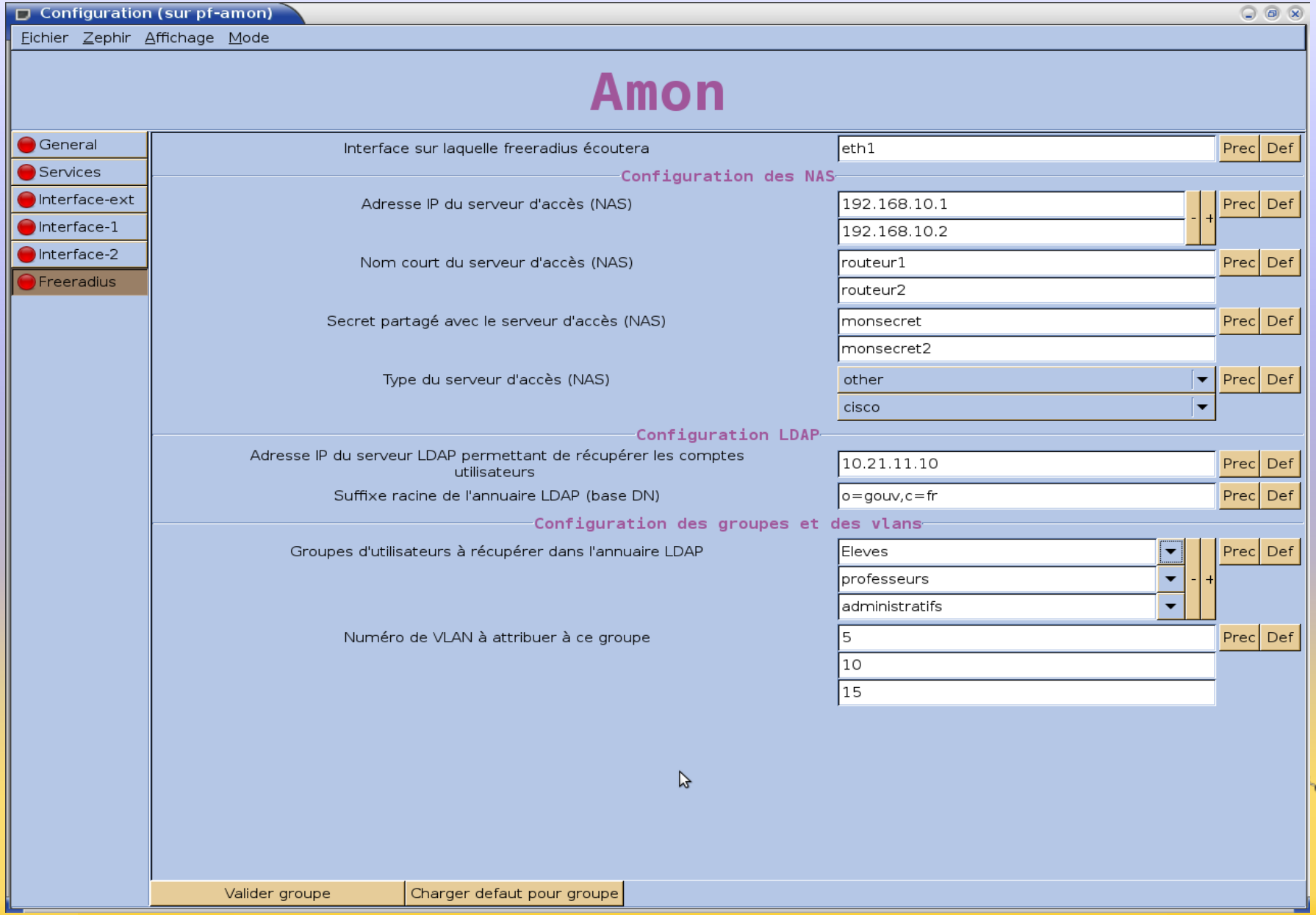
L'authentification se base sur un annuaire ldap présent en établissement.

Le paramétrage s'effectue lors de la phase de configuration du serveur (gen_config)

Permet de définir :

- les numéros de Vlans,
- le type de NAS,
- les groupes utilisateurs.

Radius (5)


Configuration (sur pf-amon)
Fichier Zephir Affichage Mode
Amon
General
Services
Interface-ext
Interface-1
Interface-2
Freeradius
Interface sur laquelle freeradius écoutera
eth1
Prec Def
Configuration des NAS
Adresse IP du serveur d'accès (NAS)
192.168.10.1
192.168.10.2
Nom court du serveur d'accès (NAS)
routeur1
routeur2
Secret partagé avec le serveur d'accès (NAS)
monsecret
monsecret2
Type du serveur d'accès (NAS)
other
cisco
Configuration LDAP
Adresse IP du serveur LDAP permettant de récupérer les comptes utilisateurs
10.21.11.10
Suffixe racine de l'annuaire LDAP (base DN)
o=gouv,c=fr
Configuration des groupes et des vlans
Groupes d'utilisateurs à récupérer dans l'annuaire LDAP
Eleves
professeurs
administratifs
Numéro de VLAN à attribuer à ce groupe
5
10
15
Valider groupe
Charger defaut pour groupe

Radius (6)

Nécessite des équipements actifs supportant ce type de protocole.

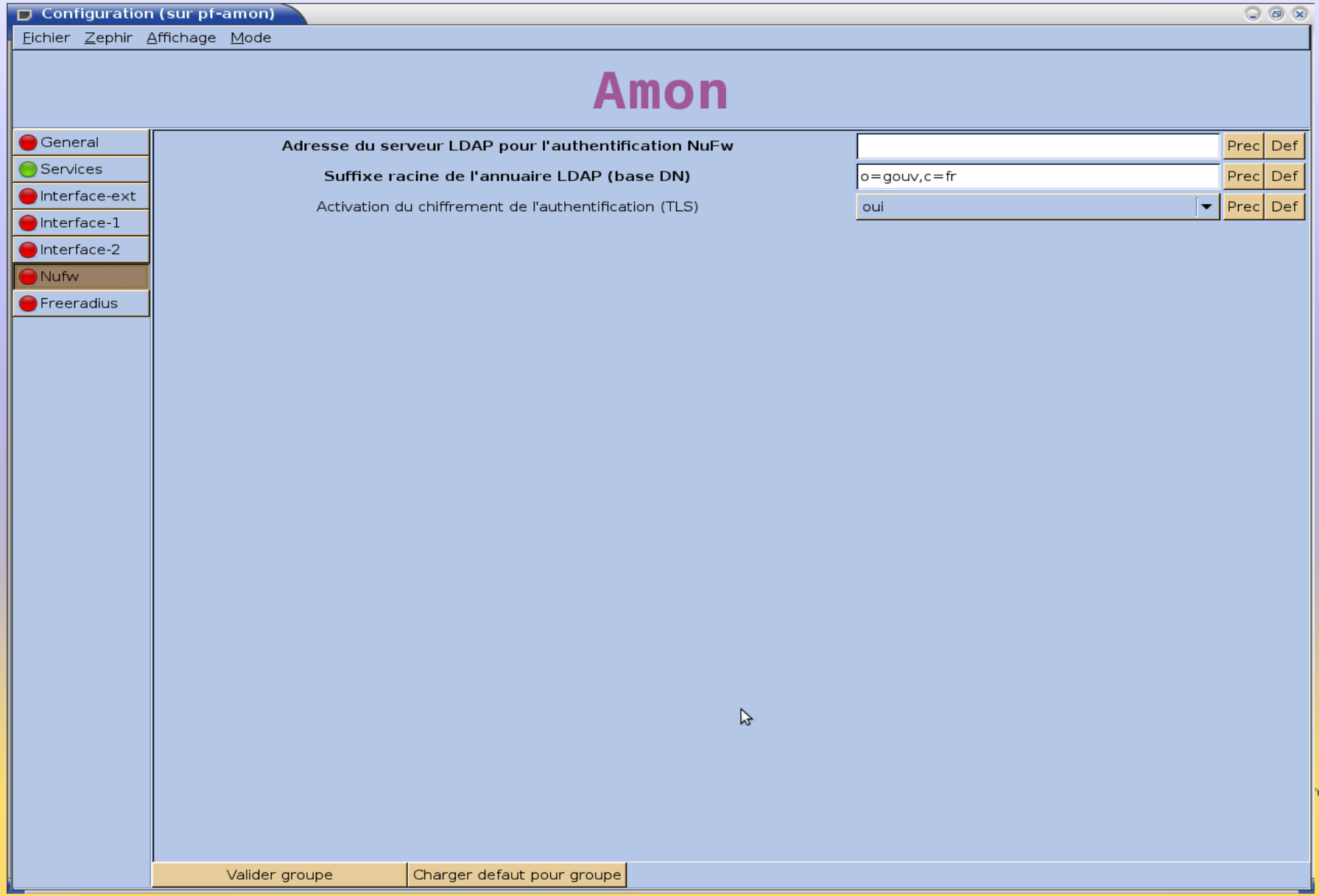
Nécessite de configurer tous les équipements du réseau.

Filtrage réseau authentifié (1)

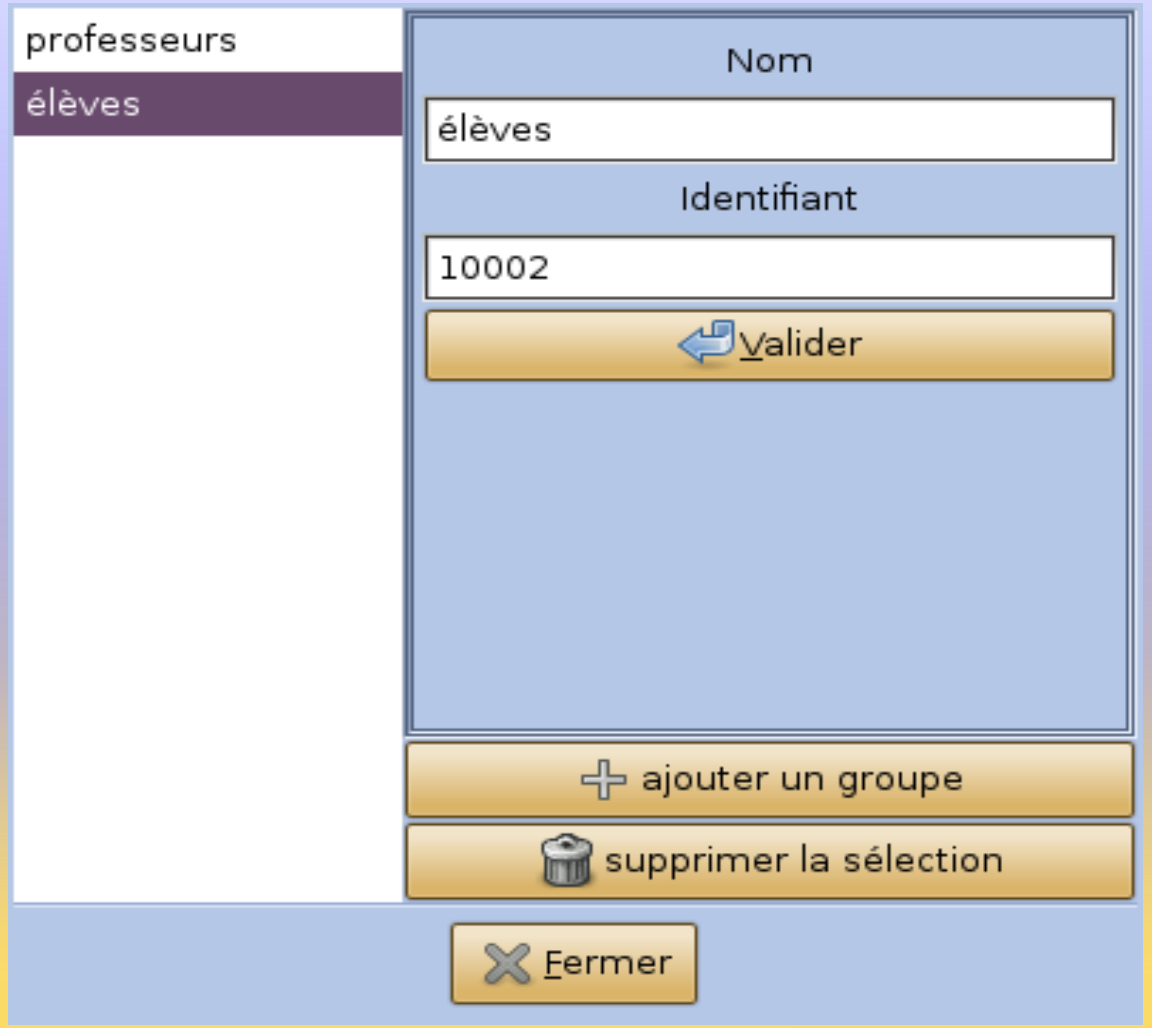
Amon permet de définir une politique de filtrage (autorisations ou interdictions) en fonction d'un groupe d'utilisateurs et/ou d'applications.

Fonctionnalité utilisable avec Era après activation de NuFW.

Filtrage réseau authentifié (2)

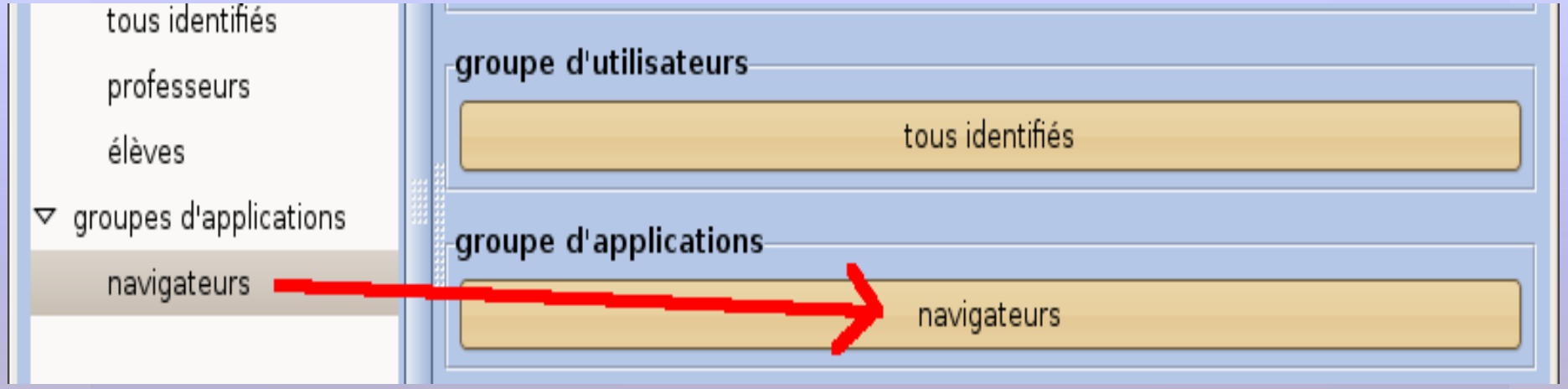


Filtrage réseau authentifié (3)



Filtrage réseau authentifié (4)

Filtrage réseau authentifié (5)

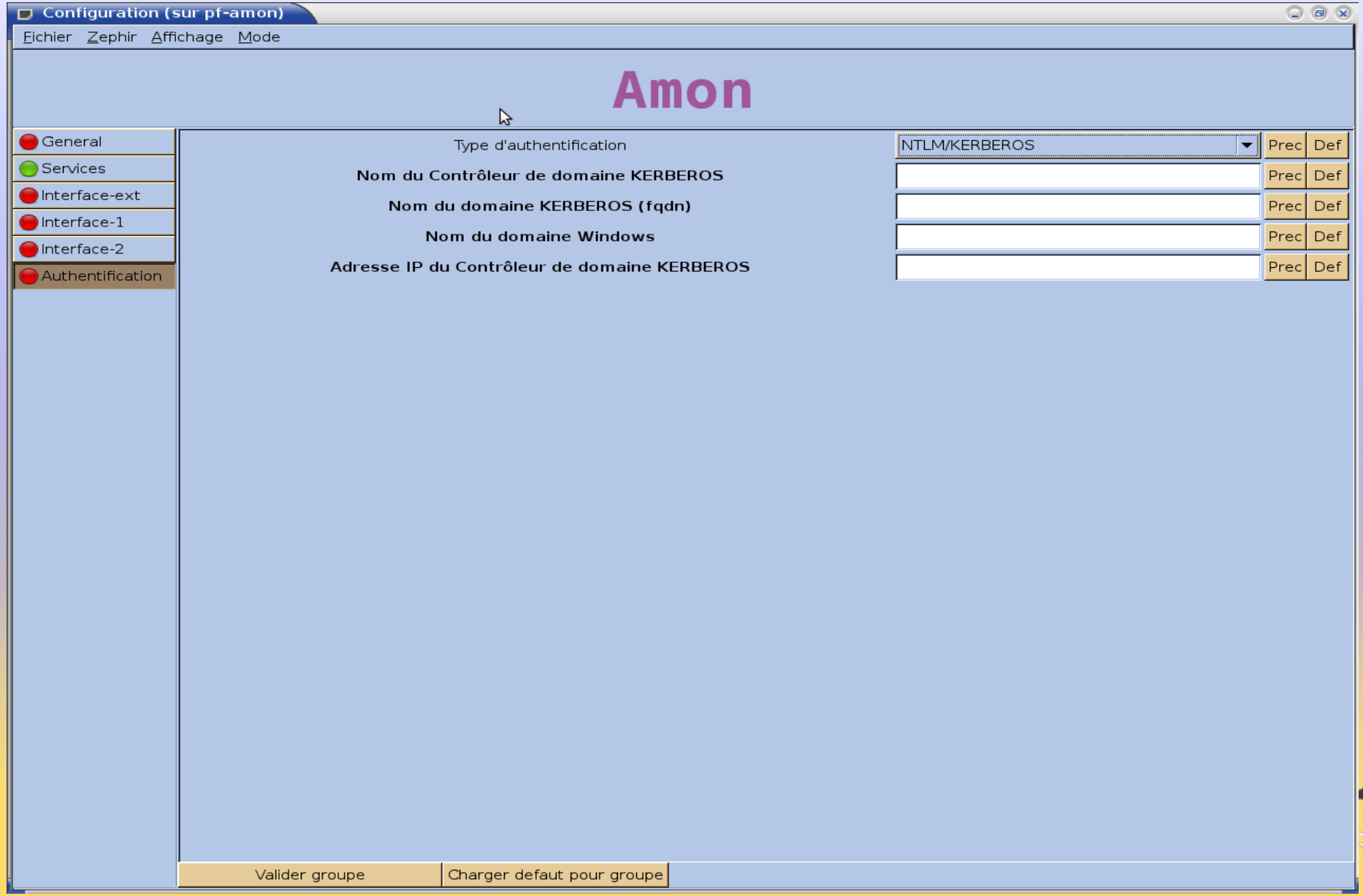


NTLM – Kerberos (1)

Amon intègre une fonctionnalité d'authentification web multi-domaine en utilisant le système de tickets Kerberos.

Assure la compatibilité avec les contrôleurs de domaines de type Windows 2003/2008 Server et Active Directory.

NTLM – Kerberos (2)



Merci de votre attention