



# **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 acs des Vlans sont les mêmes que les acs 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) | Eichier Zephyr 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:

Adresse IP de la carte externe:

Masque de sous réseau de la carte externe:

Adresse réseau de la carte externe:

Adresse Broadcast de sous réseau de la carte externe:

**Administration distante sur l'interface**

Autoriser les connexions pour administrer le serveur sur cette interface (Ead, ssh):

Adresse IP réseau autorisée à se connecter à l'interface externe:

Masque du sous réseau associé à l'IP:

**Configuration des alias sur l'interface**

Ajouter des IP alias sur l'interface:

**Configuration des vlans sur l'interface**

Activer le support des vlan sur l'interface:

Numéro d'identifiant du vlan:

Adresse IP de l'interface dans ce vlan:

Masque de sous réseau de l'interface dans ce vlan:

Adresse réseau de l'interface dans ce vlan:

Adresse de broadcast de l'interface dans ce vlan:

Adresse de la passerelle pour ce vlan. Optionnelle, uniquement si multi-routeur ("Aucun" si rien):



# Vlans (3)

Tableau des flux (sur pf-amon)

Eichier Bibliothèque Zéphir Aide

Nouveau Ouvrir Enregistrer Ajouter une zone Générer

exterieur pedago admin bastion

exterieur pedago admin bastion

exterieur 7 directives

pedago 2 directives 0 directive

admin 2 directives 0 directive 0 directive

bastion 0 directive 0 directive 0 directive

2 directives

5 directives

5 directives

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)

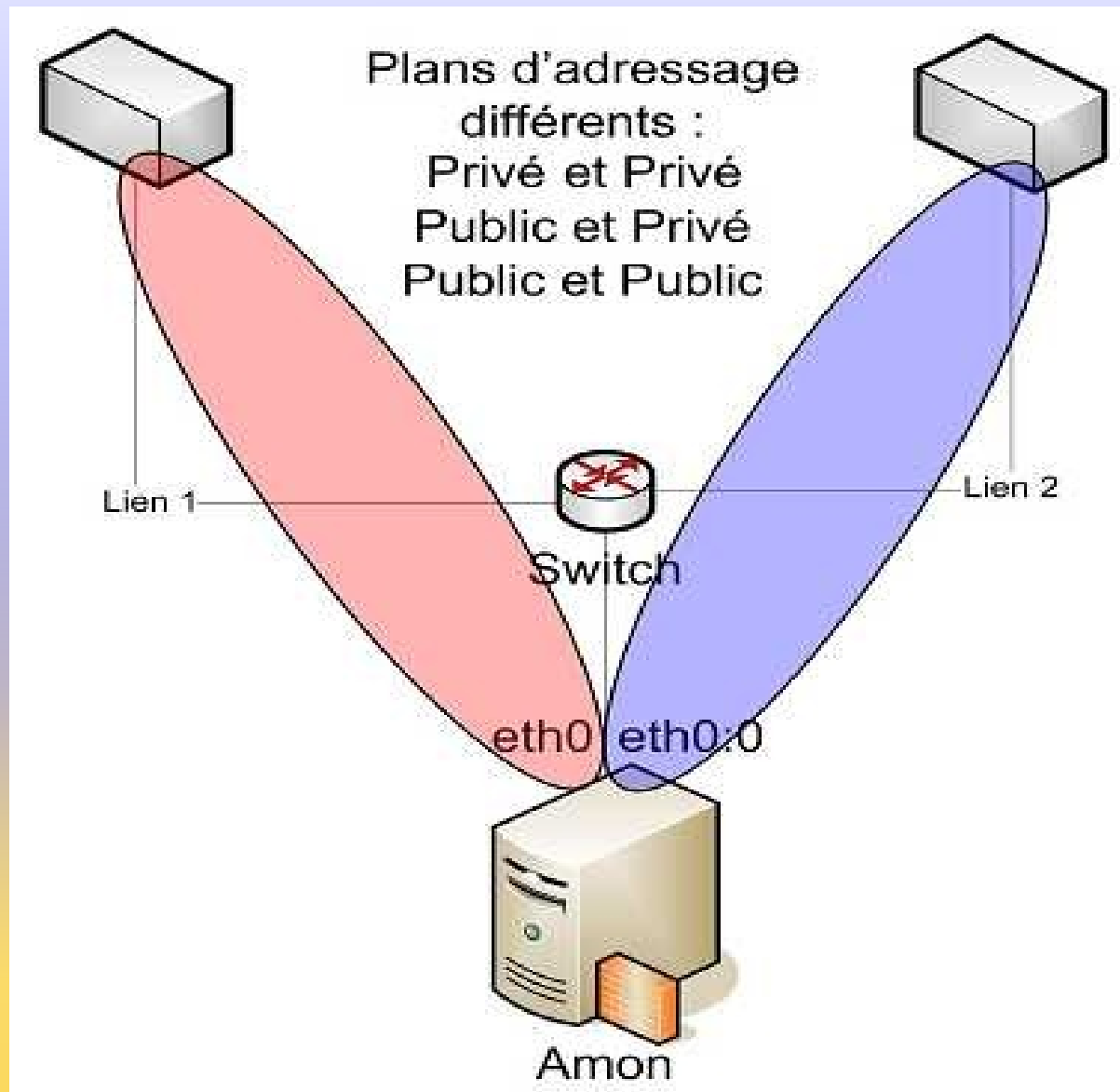
Intégration de travaux effectués par les académies de Versailles, de Nantes et de Créteil.

Permet d'utiliser 2 abonnements Internet afin de garantir une meilleure 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)

Configuration

Fichier Zephir Affichage Mode

## Amon

- General
- Services
- Interface-ext**
- Interface-1
- Interface-2
- Interface-3
- Rvp
- Prelude
- Pare-feu ac-nantes
- Dhcp

methode d'attribution de l'adressage pour l'interface: statique

**Adresse ip de la carte externe**: 195.221.64.34

**Masque de sous reseau de la carte externe**: 255.255.255.248

**Adresse réseau de la carte externe**: 195.221.64.32

**Adresse Broadcast de sous reseau de la carte externe**: 195.221.64.39

**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 externe**: 195.83.167.0

**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: oui

**Adresse ip Alias pour l'interface externe**: 10.144.250.254

**Masque de sous reseau correspondant a cet alias**: 255.255.255.252

**Adresse reseau correspondant a cet alias**: 10.144.250.252

**Adresse broadcast correspondant a cet alias**: 10.144.250.255

**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?: non

Valider groupe | Charger default pour groupe



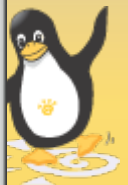
# Agrégation de Liens (5)

Configuration
\_ □ ×

Amon

Agrégation de liens

Repartition de charges entre 2 lignes ( agregation )	<input style="width: 100%;" type="text" value="oui avec alias eth0:0"/> <span style="float: right;"> <input type="button" value="Prec"/> <input type="button" value="Def"/> </span>
Lien 1	
Destination(s) forcees sur le lien 1 ( ag_force_eth0 )	<input style="width: 100%;" type="text" value="195.83.167.27"/> <span style="float: right;"> <input type="button" value="-"/> <input type="button" value="+"/> <input type="button" value="Prec"/> <input type="button" value="Def"/> </span>
Adresse(s) du(des) dns sur le lien 1 ( ag_dns_eth0 )	<input style="width: 100%;" type="text" value="80.82.224.132"/> <span style="float: right;"> <input type="button" value="-"/> <input type="button" value="+"/> <input type="button" value="Prec"/> <input type="button" value="Def"/> </span>
	<input style="width: 100%;" type="text" value="80.82.224.68"/> <span style="float: right;"> <input type="button" value="-"/> <input type="button" value="+"/> </span>
Debit mesure sur le lien 1 (entier en Mbps) ( ag_weight_eth0 )	<input style="width: 100%;" type="text" value="1"/> <span style="float: right;"> <input type="button" value="Prec"/> <input type="button" value="Def"/> </span>
Lien 2	
Destination(s) forcees sur le lien 2 ( ag_force_eth0_0 )	<input style="width: 100%;" type="text"/> <span style="float: right;"> <input type="button" value="-"/> <input type="button" value="+"/> <input type="button" value="Prec"/> <input type="button" value="Def"/> </span>
Adresse(s) du(des) dns sur le lien 2 ( ag_dns_eth0_0 )	<input style="width: 100%;" type="text" value="194.2.0.20"/> <span style="float: right;"> <input type="button" value="Prec"/> <input type="button" value="Def"/> </span>
	<input style="width: 100%;" type="text" value="195.83.167.1"/> <span style="float: right;"> <input type="button" value="-"/> <input type="button" value="+"/> </span>
	<input style="width: 100%;" type="text" value="195.83.167.2"/> <span style="float: right;"> <input type="button" value="-"/> <input type="button" value="+"/> </span>
Passerelle par defaut du lien 2 ( ag_gw_eth0_0 )	<input style="width: 100%;" type="text" value="10.144.250.253"/> <span style="float: right;"> <input type="button" value="Prec"/> <input type="button" value="Def"/> </span>
Adresse ip publique du lien 2 ( ag_ip_pub_eth0_0 )	<input style="width: 100%;" type="text" value="80.13.146.2"/> <span style="float: right;"> <input type="button" value="Prec"/> <input type="button" value="Def"/> </span>
Debit mesure sur le lien 2 (entier en Mbps) ( ag_weight_eth0_0 )	<input style="width: 100%;" type="text" value="2"/> <span style="float: right;"> <input type="button" value="Prec"/> <input type="button" value="Def"/> </span>
Divers	
Delai entre les tests d etat (en secondes) ( ag_pause )	<input style="width: 100%;" type="text" value="10"/> <span style="float: right;"> <input type="button" value="Prec"/> <input type="button" value="Def"/> </span>
TimeOut de la requete DNS (en secondes) ( ag_timeout )	<input style="width: 100%;" type="text" value="1"/> <span style="float: right;"> <input type="button" value="Prec"/> <input type="button" value="Def"/> </span>
Premiere Adresse DNS testee ( ag_testdns )	<input style="width: 100%;" type="text" value="www.google.com"/> <span style="float: right;"> <input type="button" value="Prec"/> <input type="button" value="Def"/> </span>
Seconde Adresse DNS testee ( ag_testdns2 )	<input style="width: 100%;" type="text" value="www.ac-nantes.fr"/> <span style="float: right;"> <input type="button" value="Prec"/> <input type="button" value="Def"/> </span>
Nombre de succes avant changement d etat ( ag_nbsucces )	<input style="width: 100%;" type="text" value="4"/> <span style="float: right;"> <input type="button" value="Prec"/> <input type="button" value="Def"/> </span>
Nombre d echecs avant changement d etat ( ag_nbechecs )	<input style="width: 100%;" type="text" value="1"/> <span style="float: right;"> <input type="button" value="Prec"/> <input type="button" value="Def"/> </span>



# 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	<input type="checkbox"/>
netbios	<input checked="" type="checkbox"/>





# 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.

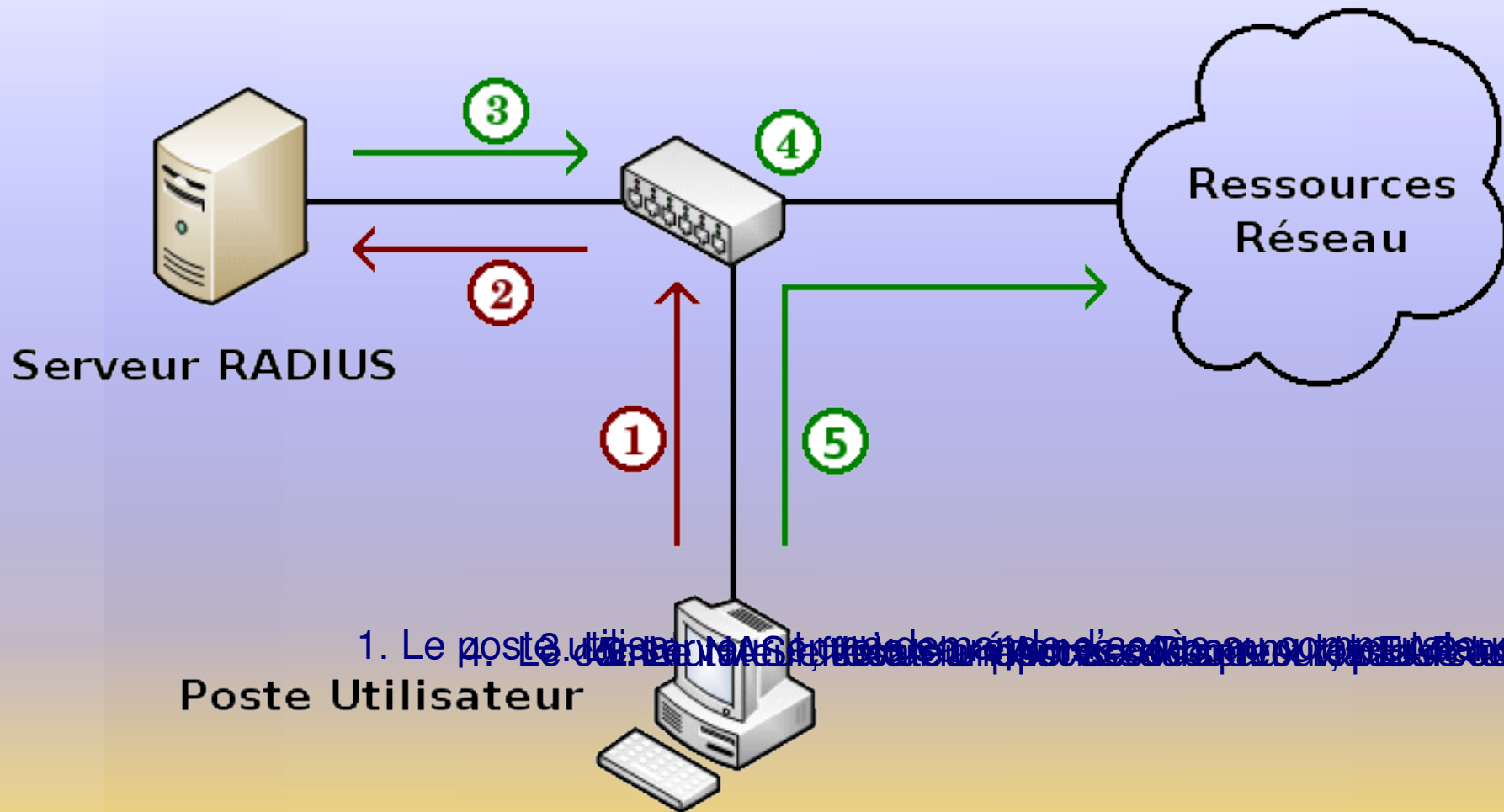
Intégration des postes nomades (portables, etc.)

Prise en compte des connexions sans fils.





# Radius (3)



1. Le poste utilisateur demande un accès à un service réseau.  
Le serveur RADIUS est informé de la demande et vérifie les droits de l'utilisateur.





## 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 Vlan,

- le type de NAS,

- les groupes utilisateurs.



# Radius (5)

Configuration (sur pf-amon) Echier Zephir Affichage Mode

## Amon

- General
- Services
- Interface-ext
- Interface-1
- Interface-2
- Freeradius

Interface sur laquelle freeradius écoutera	eth1	Prec Def
<b>Configuration des NAS</b>		
Adresse IP du serveur d'accès (NAS)	192.168.10.1	Prec Def
	192.168.10.2	- +
Nom court du serveur d'accès (NAS)	routeur1	Prec Def
	routeur2	
Secret partagé avec le serveur d'accès (NAS)	monsecret	Prec Def
	monsecret2	
Type du serveur d'accès (NAS)	other	Prec Def
	cisco	
<b>Configuration LDAP</b>		
Adresse IP du serveur LDAP permettant de récupérer les comptes utilisateurs	10.21.11.10	Prec Def
Suffixe racine de l'annuaire LDAP (base DN)	o=gouv,c=fr	Prec Def
<b>Configuration des groupes et des vlans</b>		
Groupes d'utilisateurs à récupérer dans l'annuaire LDAP	Eleves	Prec Def
	professeurs	- +
	administratifs	
Numéro de VLAN à attribuer à ce groupe	5	Prec Def
	10	
	15	





## 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)

Configuration (sur pf-amon)

Echier Zephir Affichage Mode





## Amon

<input type="radio"/> General	Adresse du serveur LDAP pour l'authentification NuFw	<input type="text"/>	Prec	Def
<input type="radio"/> Services	Suffixe racine de l'annuaire LDAP (base DN)	<input type="text" value="o=gouv,c=fr"/>	Prec	Def
<input type="radio"/> Interface-ext	Activation du chiffrement de l'authentification (TLS)	<input type="text" value="oui"/>	Prec	Def
<input type="radio"/> Interface-1				
<input type="radio"/> Interface-2				
<input checked="" type="radio"/> Nufw				
<input type="radio"/> Freeradius				

Valider groupe | Charger default pour groupe



# Filtrage réseau authentifié (3)

professeurs	Nom
élèves	élèves
	Identifiant
	10002
	 Valider
	 ajouter un groupe
	 supprimer la sélection
 Fermer	



# Filtrage réseau authentifié (4)





# Filtrage réseau authentifié (5)

The screenshot displays a web interface for network filtering. On the left, a vertical menu lists categories: 'tous identifiés', 'professeurs', 'élèves', 'groupes d'applications' (with a dropdown arrow), and 'navigateurs'. The 'navigateurs' item is highlighted with a grey background. A red arrow points from this item to the right-hand panel. The right panel is titled 'groupe d'utilisateurs' and 'groupe d'applications'. Under 'groupe d'utilisateurs', there is a yellow button labeled 'tous identifiés'. Under 'groupe d'applications', there is a yellow button labeled 'navigateurs', which is also pointed to by the red arrow.





## 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.



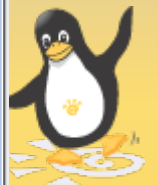
# NTLM – Kerberos (2)

Configuration (sur pf-amon)

Eichier Zephyr Affichage Mode

## Amon

<ul style="list-style-type: none"> <li><input type="radio"/> General</li> <li><input type="radio"/> Services</li> <li><input type="radio"/> Interface-ext</li> <li><input type="radio"/> Interface-1</li> <li><input type="radio"/> Interface-2</li> <li><input checked="" type="radio"/> Authentification</li> </ul>	<p>Type d'authentification</p> <p>Nom du Contrôleur de domaine KERBEROS</p> <p>Nom du domaine KERBEROS (fqdn)</p> <p>Nom du domaine Windows</p> <p>Adresse IP du Contrôleur de domaine KERBEROS</p>	<table border="1"> <tr> <td>NTLM/KERBEROS</td> <td>Prec</td> <td>Def</td> </tr> <tr> <td></td> <td>Prec</td> <td>Def</td> </tr> <tr> <td></td> <td>Prec</td> <td>Def</td> </tr> <tr> <td></td> <td>Prec</td> <td>Def</td> </tr> <tr> <td></td> <td>Prec</td> <td>Def</td> </tr> </table>	NTLM/KERBEROS	Prec	Def		Prec	Def		Prec	Def		Prec	Def		Prec	Def
NTLM/KERBEROS	Prec	Def															
	Prec	Def															
	Prec	Def															
	Prec	Def															
	Prec	Def															





**Merci de votre attention**

