Installation et mise en œuvre du module Amon

EOLE 2.5.2

création : Mai 2015 Version : révision : Novembre 2016

EOLE 2.5.2

Version : révision : Novembre 2016

Date : création : Mai 2015

Editeur : Pôle national de compétences Logiciels Libres

Auteur(s) : Équipe EOLE

Pour toute information concernant ce projet vous pouvez nous joindre :

- Par courrier électronique : eole@ac-dijon.fr
- Par FAX : 03-80-44-88-10
- Par courrier : EOLE-DSI - 2G, rue du Général Delaborde - 21000 DIJON
- Le site du Pôle national de compétences Logiciels Libres : http://eole.orion.education.fr

Table des matières

Chapitre 1

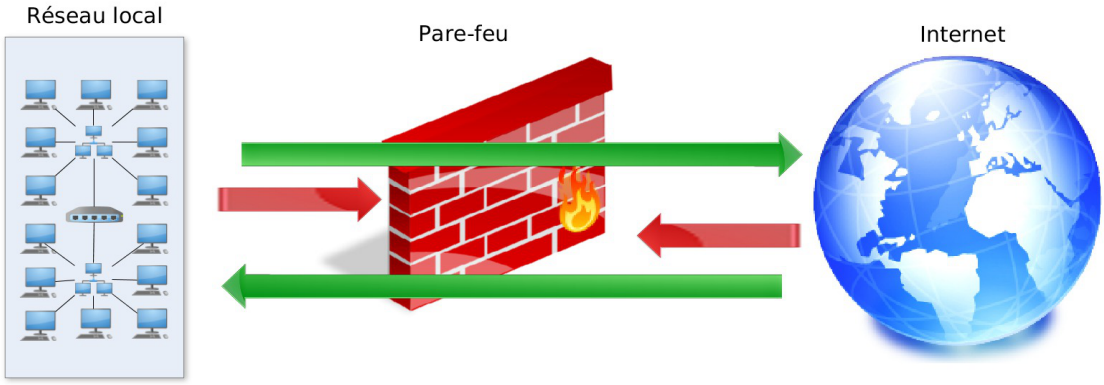
Introduction au module Amon

Le module Amon est un pare-feu facile à installer et à utiliser. Il permet de faire respecter la politique de sécurité du réseau et les types de communication autorisés. Il a pour principale tâche de contrôler le trafic entre différentes zones : Internet et le réseau interne.

Le filtrage se fait selon plusieurs critères :

- l'origine ou la destination des paquets (adresse IP, ports TCP ou UDP, interface réseau, etc.) ;
- les options contenues dans les données (fragmentation, validité, etc.) ;
- les données elles-mêmes (taille, correspondance avec un motif, etc.).

Un pare-feu permet de se prémunir des attaques extérieures.



Un pare-feu fait office de routeur, il permet donc de partager un accès Internet en toute sécurité entre les sous-réseaux d'un réseau local. Il crée un véritable intranet fédérateur au sein de votre établissement (entreprise, établissements scolaires, collectivités territoriales, association) et de n'importe quel réseau local (usage domestique).

1. Qu'est ce que le module Amon ?

Le module Amon permet de partager en toute sécurité un accès Internet entre les sous-réseaux d'un réseau local.

Installé sur un serveur dédié, équipé de deux, trois, quatre ou cinq interfaces réseau, il permet d'organiser au mieux l'architecture réseau d'un établissement.

Des modèles de règles de pare-feu sont disponibles pour chaque architecture.

Vous pouvez les utiliser tels quels ou bien les modifier à votre convenance. Un outil spécifique, ERA[p.305], est à votre disposition pour effectuer ce travail.

Il est également possible de créer un réseau virtuel privé (RVP[p.312], VPN) entre l'établissement (une structure administrative) et un concentrateur académique (par exemple le module Sphynx). Ce réseau virtuel privé permet de sécuriser les flux sensibles au travers d'Internet.

Pour l'Éducation nationale, ce réseau est nommé réseau AGRIATES[p.301] .

Le module Amon assure uniquement des services liés à la sécurité : il doit être installé sur un serveur dédié.

Pour installer plusieurs modules sur un même serveur il est possible d'utiliser les modules AmonEcole, AmonHorus et AmonEcole+.

Principales fonctionnalités :

- routage ;
- authentification des utilisateurs ;
- filtrage IP ;
- filtrage de site amélioré (listes noires et contenu) ;
- réseau virtuel privé ;
- suivi détaillé de la navigation web ;
- mises à jour automatiques ;
- journalisation des fichiers logs ;
- détection d'intrusions ;
- service de cache web ;
- administration simplifiée ;
- statistiques sur l'état du système ;
- statistiques d'utilisation.

2. À qui s'adresse ce module ?

Le module Amon s'adresse à toutes les structures pourvues d'un réseau interne communiquant avec l'extérieur :

- entreprises ;
- établissements scolaires ;
- collectivités territoriales ;
- associations ;
- etc.

Le module Amon s'adresse à toutes les structures désireuses d'accroître la sécurité de leurs réseaux :

- de protéger leur réseau interne et/ou le découper en sous-réseaux ;
- de réguler les accès réseau vers l'extérieur ;
- de sécuriser la navigation sur le web.

Le module Amon peut être utilisé pour un usage domestique.

3. Les services Amon

Chaque module EOLE est constitué d'un ensemble de services.

Chacun de ces services peut évoluer indépendamment des autres et fait l'objet d'une actualisation ou d'une intégration par l'intermédiaire des procédures de mise à jour. Ce qui permet d'ajouter de nouvelles fonctionnalités ou d'améliorer la sécurité.

Services communs à tous les modules

- *Noyau Linux 3.x* : Noyau Linux Ubuntu ;
- *OpenSSH* : prise en main à distance moyennant une demande d'authentification ;
- *Rsyslog* : service de journalisation et de centralisation des logs ;
- *Pam* : gestion des authentifications ;
- *EAD* : outil EOLE pour l'administration du serveur ;
- *EoleSSO* : gestion de l'authentification centralisée ;
- *Exim4* : serveur de messagerie ;
- *NUT* : gestion des onduleurs ;
- *NTP* : synchronisation avec les serveurs de temps.

Services spécifiques au module Amon

- *Bind* : implémentation la plus répandue du DNS (résolution des noms de machine en adresse IP) ;
- *iptables* : filtrage d'adresses IP ;
- *Squid* : proxy cache qui permet d'accélérer les connexions Internet ;
- *e2guardian* : outil de filtrage syntaxique des adresses web ;
- *LightSquid* : générateur de statistiques pour le proxy Squid ;
- *Strongswan* : version libre d'IPSec. Permet la création de réseaux virtuels privés ;
- *NginX* : proxy inverse ;
- *FreeRADIUS* : service d'authentification réseau ;
- *ERA* : outil de génération de règles iptables.

4. Structure des conteneurs

Le module Amon s'installe par défaut en mode non conteneur[p.303].

La mise en œuvre du mode conteneur pour ce module est possible mais ne fait pas l'objet d'une procédure de qualification.

5. Pré-requis

Le module Amon assure uniquement des services liés à la sécurité : il doit être installé sur un serveur dédié.

Ce module fonctionne relativement bien sur de petits serveurs mais l'espace disque, la mémoire et la vitesse du CPU doivent être adaptés au nombre de connexions simultanées.

Les CPU doivent être de préférence en 64 bits.

Le modèle de filtrage est déterminé par le nombre de carte lui même dépendant de l'utilisation que vous faites du serveur.

Dans la plupart des cas le module Amon est équipé de 4 cartes réseau :

- réseau extérieur ;
- réseau interne pédagogique ;
- réseau interne administratif ;
- une DMZ[p.304].

L'espace disque et la mémoire RAM sont les ressources les plus critiques, lors d'un partitionnement manuel il faut privilégier la partition `/var` qui contient le plus de données.

Exemple d'usage du module Amon dans un collège. Il y a environ 200 comptes utilisateurs, 140 postes clients et 50 connectés en moyenne. Cette machine est un Intel(R) Xeon(R) CPU X3430 @ 2.40GHz avec 2Go de RAM et 30Go d'espace disque (dont 20 Go sont réservés au `/var` et utilisé à 50%).

6. Les différences entre les versions 2.4 et 2.5

La version 2.5 du module Amon n'est disponible qu'à partir de la version 2.5.1 d'EOLE.

La nouvelle version du module reproduit les mêmes fonctionnalités (iso-fonctionnel) que la version 2.4. La version 2.5 est basée sur une nouvelle version LTS d'Ubuntu.

Noyau

Cette nouvelle version d'Ubuntu implique également un changement de version du noyau avec de nouvelles prises en charge matériel. Les modules EOLE 2.5 utilisent par défaut le noyau le plus récent de la distribution Ubuntu.

Mise à jour

Sur EOLE 2.5, il n'existe plus qu'un seul niveau de mise à jour, le concept de mise à jour minimale et complète a été supprimé.

Les mises à jour sont automatiques mais peuvent se faire manuellement avec la commande `Maj-Auto`.

Passage à une nouvelle version

L'ajout de nouvelles fonctionnalités entraîne une nouvelle version d'EOLE (2.5.n). Le passage d'une version mineure à une autre est manuel et volontaire.

La commande `Maj-Release` permet de passer à une version mineure plus récente.

Le passage à une nouvelle version d'Ubuntu entraîne une nouvelle version d'EOLE (2.n.n). Le passage d'une version majeure à une autre est manuel et volontaire.

La commande `Upgrade-Auto` permet de passer à une version majeure supérieure.

Commandes

Les commandes `instance`, `reconfigure` et `Maj-Auto` ainsi que la gestion des services ont été réécrites. La commande `diagnose` a été enrichie.

Il n'est plus nécessaire de spécifier le nom du fichier à utiliser pour les commandes `instance` et `reconfigure`.

Un fichier `config.eol.bak` est généré dans le répertoire `/etc/eole/` à la fin de l'instanciation et à la fin de la reconfiguration du serveur. Celui-ci permet d'avoir une trace de la dernière configuration fonctionnelle du serveur.

Interface de configuration du module

L'interface de configuration du module est basée sur de nouvelles technologies :

- Flask[p.305] ;
- Backbone.js[p.302] et Marionette[p.307] ;
- Tiramisu[p.313].

Elle peut être rendue disponible au travers d'un navigateur web.

Il n'est plus nécessaire de spécifier le nom du fichier à utiliser avec les commandes `gen_config` et `instance`.

Règles pare-feu

La gestion des règles pare-feu ne se fait plus par fichiers `.fw`. Les règles sont maintenant définies dans des dictionnaires XML Creole.

Les flux réseau ne sont plus bloqués en interne (entre le maître et les conteneurs et entre conteneurs).

Tâches planifiées

Sur les modules EOLE, les tâches planifiées (comme par exemple les mises à jour) sont gérées par `eole-schedule`.

En version 2.5, `eole-schedule` est géré depuis Tiramisu[p.313].

La liste des scripts à activer pour la gestion des tâches est décrite dans des dictionnaires XML[p.314] Creole extra. Ce système permet de mettre en place des valeurs par défaut. Ainsi, l'activation ou la désactivation d'un script n'est plus réalisée à l'installation du paquet associé ce qui est à la fois plus simple et plus sûr.

Mode conteneur

Pour les modules en mode conteneur il n'est plus possible de personnaliser le réseau des conteneurs avec l'option `-n`.

Pour passer un module en mode conteneur le paquet à installer est `eole-lxc-controller`.

Le mode conteneur utilise dorénavant le service `apt-cacher` pour mettre en cache les paquets Debian. Le service est installé sur le maître et est utilisé par le maître et les conteneurs LXC.

La nouvelle version LXC sur Ubuntu 14.04 entraîne une simplification de la gestion des conteneurs

Changement dans le PATH des commandes

Beaucoup de commandes n'ont plus besoin du chemin absolu pour être exécutées.

Répertoire d'installation du logiciel Nginx

Le répertoire d'installation du logiciel nginx n'est plus `/usr/share/nginx/www/` mais `/usr/share/nginx/html/`

Suppression de la base matériels

La base des matériels maintenue par EOLE a été supprimée, cette base n'était plus pertinente car elle pouvait contenir du matériel inutilisé comme étant compatible avec les modules EOLE.

Logiciel de sauvegarde

Sur les modules 2.5 le logiciel Bareos remplace le logiciel Bacula.

2.5.1

Filtrage avec e2guardian

Le module Amon intègre le logiciel libre e2guardian[p.304]. Le logiciel DansGuardian a été complètement abandonné sur le module. Le nombre maximum de processus disponibles pour traiter les nouvelles

connexions peut être modifié jusqu'à 8192.

WPAD

WPAD supporte les VLAN et les alias, Nginx renvoie le bon fichier WPAD si des VLAN ou des alias sont déclarés.

Il est également possible de changer le port du proxy diffusé par défaut pour une interface, un VLAN ou un alias donné.

Paquet dédié pour le service WPAD d'EOLE

Un paquet nommé `eole-wpad` est nouvellement dédié pour gérer la découverte automatique du proxy par les navigateurs.

Mode VPN

Le mode VPN database n'est plus supporté et n'est plus disponible sur le module Amon.

2.5.2

Mot de passe au 1er redémarrage après installation

Une fois le système redémarré, comme indiqué par le prompt, vous pouvez ouvrir une session en console, mais aussi par SSH, avec l'utilisateur **root** et le **mot de passe aléatoire** qui est **affiché**.

Liste des domaines de destination à ne pas authentifier

La gestion de la liste des domaines de destination à ne pas authentifier est prise en charge dans l'interface de configuration du module.

7. Errata 2.5.n

Il n'y a plus qu'un seul niveau de mise à jour qui comportera uniquement les « bugs » critiques et les correctifs de sécurité. Les mises à jour automatiques ne contiennent pas de changement fonctionnel.

Les modifications et ajouts de fonctionnalités font l'objet d'une nouvelle version fonctionnelle (2.X.Y) et la mise à niveau s'effectue avec une procédure automatique distincte de la mise à jour ordinaire.

Quand une correction nécessite une modification sur les template et/ou les dictionnaires, elle n'est pas intégrée aux versions fonctionnelles déjà diffusées en stable afin de préserver l'intégrité des patch effectués par chacun d'entre vous.

Une page d'errata recense des problèmes affectant chacune des versions EOLE 2.5.x. Les dysfonctionnement connus sont corrigés d'une version à une autre d'EOLE.

http://dev-eole.ac-dijon.fr/projects/modules-eole/wiki/Errata25

Le tableau contient les informations permettant d'appliquer manuellement les correctifs aux versions antérieures à la colonne `Corrigé à partir de`, vous permettant ainsi de les intégrer à vos patch existants si besoin.

Chapitre 2

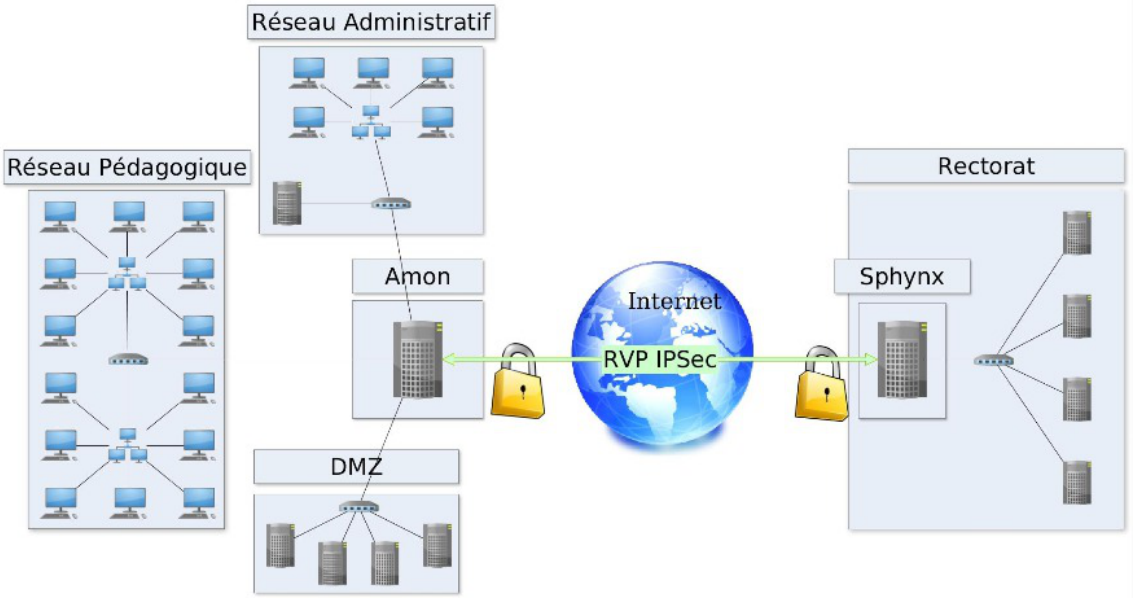
Fonctionnement du module Amon

Pour jouer son rôle, le module Amon repose sur beaucoup de projets libres : iptables, strongSwan, squid, e2guardian, Nginx.

Tous les services sont activables, désactivables, pour construire une passerelle sur mesure.

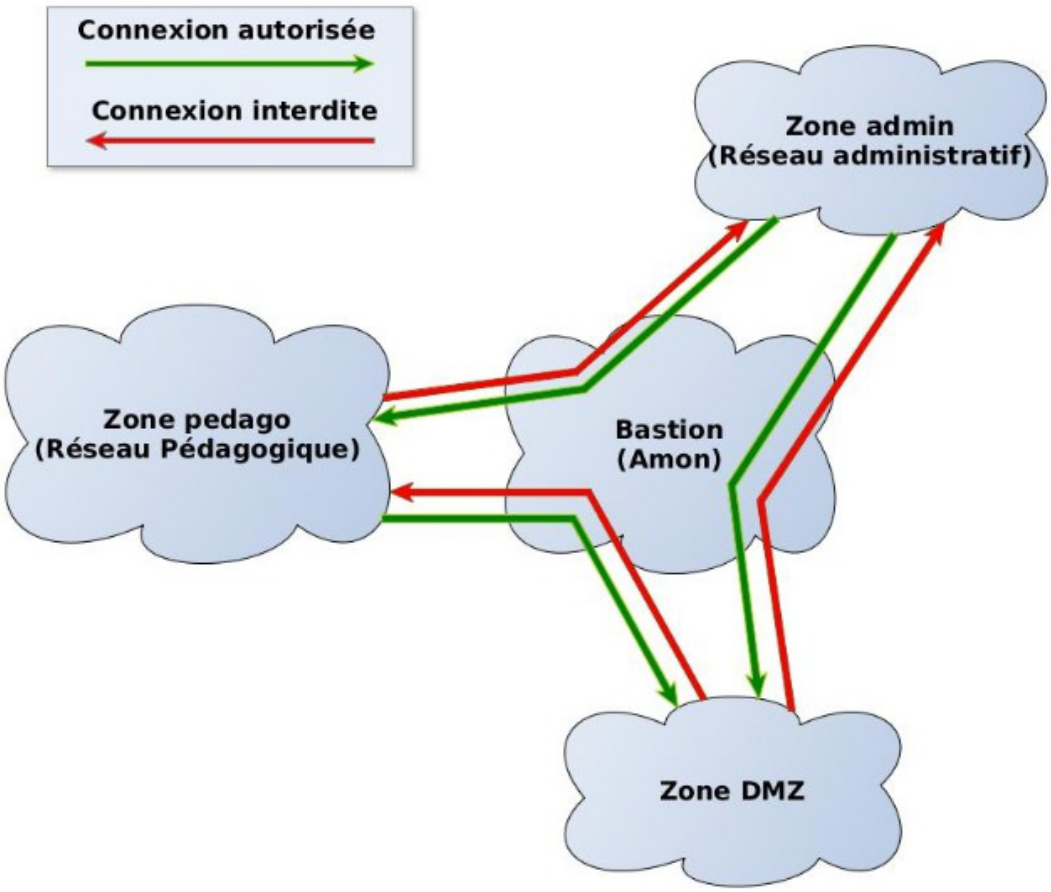
La passerelle permet :

- la mutualisation de l'accès Internet pour les réseaux locaux ;
- la gestion des Réseaux Virtuels Privés (RVP/VPN).



Le module Amon permet de mettre en place rapidement et facilement tous les services nécessaires à la sécurisation d'un réseau et à l'application des règles de communication autorisées. Le pare-feu[p.310] repose sur le logiciel iptables[p.306] et l'éditeur de règles ERA[p.305] permet de générer les règles et de gérer la description de la politique de sécurité d'un pare-feu. Cette politique est sauvegardée intégralement dans un fichier de type XML[p.314] avec un format spécifique à l'application.

Par un processus de compilation, ERA transforme le fichier XML en un bloc de règles iptables, de manière à instancier ces règles sur un pare-feu cible.



Typiquement, le module Amon devrait être équipé au minimum de 2 cartes réseau :

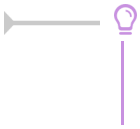
- l'interface-0, carte affectée pour le trafic réseau extérieur ;
- l'interface-1, carte affectée pour le trafic réseau intérieur ;

Des cartes supplémentaires interface-n peuvent être ajoutées.

Les modèles de zone par défaut proposés supportent jusqu'à 5 cartes réseau :

- **2zones** : gestion d'une zone admin ou pedago sur eth1 ;
- **2zones-amonecole** : modèle spécifique au module AmonEcole (pedago sur eth1) ;
- **3zones** : gestion d'une zone admin sur eth1 et d'une zone pedago sur eth2 ;
- **3zones-dmz** : gestion d'une zone pedago sur eth1 et d'une zone DMZ publique pouvant accueillir un module Scribe sur eth2 ;
- **4zones** : gestion d'une zone admin sur eth1, d'une zone pedago sur eth2 et d'une zone DMZ publique pouvant accueillir un module Scribe sur eth3 ;
- **5zones** : gestion d'une zone admin sur eth1, d'une zone pedago sur eth2, d'une zone DMZ publique pouvant accueillir un module Scribe sur eth3 et d'une zone DMZ privée sur eth4.

Le modèle de zone proposés correspondent à un modèle de filtrage ERA. Les modèles de filtrage ERA sont la description de pare-feu enregistrés dans des fichiers XML situés par défaut dans le répertoire `/usr/share/era/modeles/`.



Avec ERA il est possible de créer un nouveau modèle personnalisé dans le répertoire `/usr/share/era/modeles/`. Celui-ci apparaîtra dans la liste des modèles proposés par défaut.

Chaque carte réseau devra avoir sa propre adresse IP. Le choix de celles-ci dépend de l'architecture réseau en place.

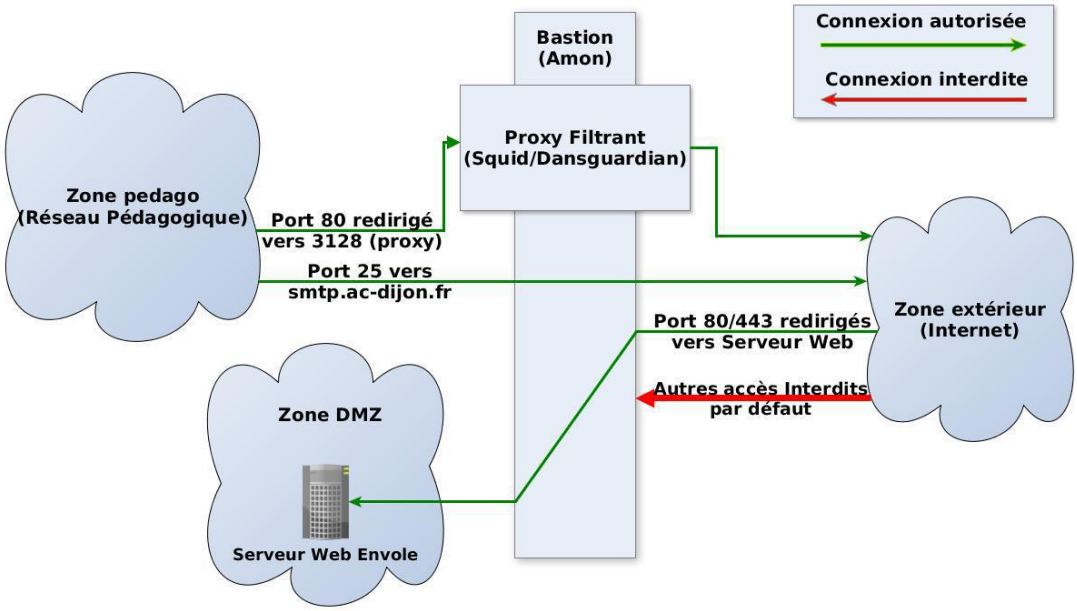
Le service bastion récupère les règles par défaut des zones ainsi que toutes les règles personnalisées :

- les règles optionnelles de l'EAD ;
- les postes et les groupes de postes interdits ou restreints dans l'EAD ;
- les règles sur les horaires de l'EAD ;
- les règles ipsets (les exceptions sur une directive) ;
- les règles de la QOS ;
- les règles tcpwrapper (host allow et hosts deny).

Le service bastion gère également les règles iptables dans les conteneurs lorsque le module en est pourvu.
La liste des actions du service se trouve dans le script `/usr/share/era/bastion.sh`.
Le service bastion met en cache les règles mais ne les régénère pas à chaque fois.
Seules les commandes `CreoleService bastion restart` ou `service bastion restart` vont régénérer les règles.

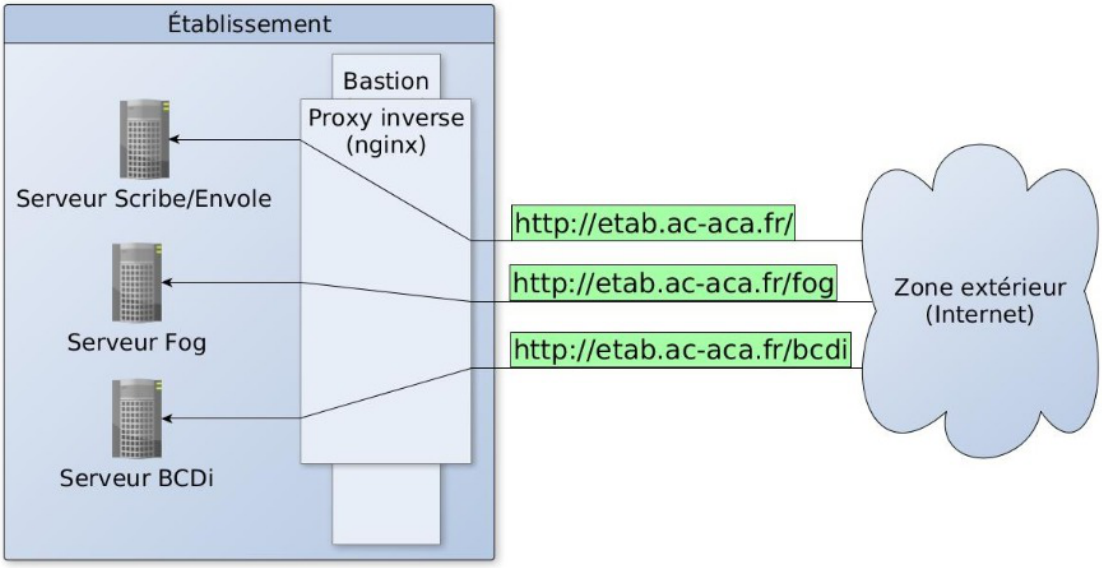
Le proxy filtrant repose sur l'utilisation de squid et de e2guardian et permet :

- de gérer une liste de sites et d'URL interdits ;
- le filtrage syntaxique ;
- l'interdiction par extension et type MIME ;
- de gérer une liste blanche (« tout interdit sauf ») ;
- d'interdire une plage d'IP et plage horaire ;
- l'économie de bande passante par la mise en cache.



Le module Amon utilise Nginx pour mettre en place un proxy inverse qui permet :

- d'ouvrir des services Web sur Internet ;
- de rediriger par URL ;
- de forcer l'utilisation de HTTPS ;
- la ré-écriture d'URL (expressions régulières).



D'autres services sont également proposés.

Parmi les plus couramment utilisés :

- l'établissement de réseaux virtuels privés ;
- la délégation de zone DNS et le DNS local reposent sur bind ;
- l'authentification Wifi repose sur le logiciel libre FreeRADIUS.

Chapitre 3

Installation du module Amon

L'installation du module **n'est pas détaillée** dans cette documentation, veuillez vous reporter à la documentation EOLE 2.5, commune aux différents modules, à la documentation sur la mise en œuvre d'un module ou à la documentation complète du module.

Après l'installation du module Amon, la mise à jour n'est pas obligatoire mais fortement recommandée.

Mise à jour

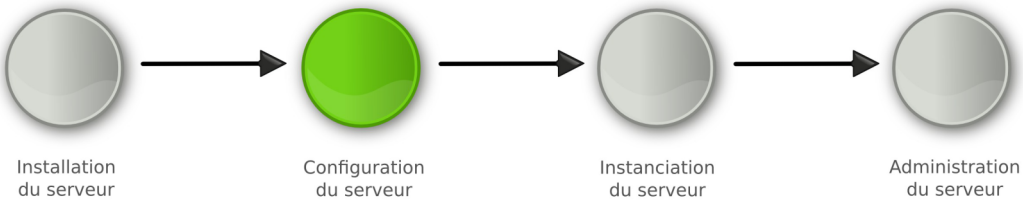
Pour effectuer la mise à jour du module, utiliser la commande : `Maj-Auto`.

Mise à jour dans le cas d'un module en mode conteneur

Le mode conteneur utilise dorénavant le service `apt-cacher` pour mettre en cache les paquets Debian. Le service est installé sur le maître et est utilisé par le maître et les conteneurs LXC.

Chapitre 4

Configuration du module Amon



Configuration

Les généralités sur la configuration **ne sont pas traitées** dans cette documentation, veuillez vous reporter à la documentation de mise en œuvre d'un module EOLE ou à la documentation complète du module.

- La **phase de configuration** s'effectue au moyen de l'interface de configuration du module, celle-ci se lance avec la commande `gen_config`.

  Cet outil permet de renseigner et de stocker en un seul fichier (`config.eol`) tous les paramètres nécessaires à l'utilisation du serveur dans son environnement (l'adresse IP de la carte eth0 est un exemple de paramètre à renseigner). Ce fichier sera utilisé lors de la phase d'instanciation.

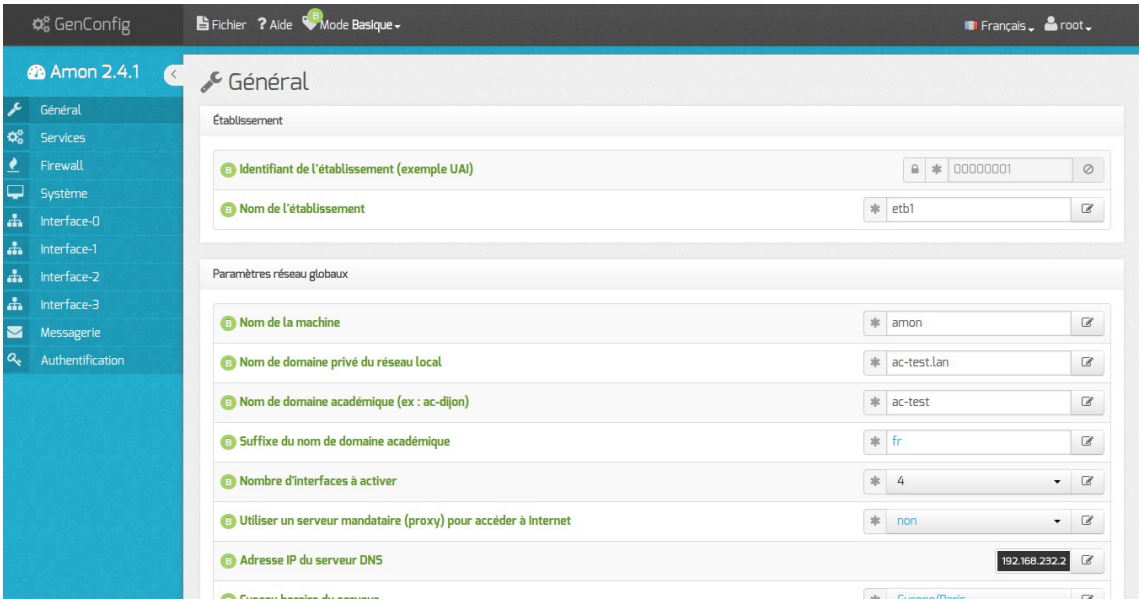
  Suivant les modules, le nombre de paramètres à renseigner est plus ou moins important.

  Cette phase de configuration peut permettre de prendre en compte des paramétrages de fichiers de configuration de produits tels que Squid[p.313], e2guardian[p.304], etc.

1. Configuration en mode basique

Dans l'interface de configuration du module voici les onglets propres à la configuration du module Amon :

- `Général` ;
- `Firewall` ;
- `Interface-0` (configuration de l'interface réseau) ;
- `Interface-1` (configuration de l'interface réseau) ;
- `Messagerie` ;
- `Authentification`.



Vue générale de l'interface de configuration du module

Dans les onglets `Général` et `Firewall`, deux options sont à renseigner avec la plus grande attention : le `Nombre d'interfaces à activer` et le `Modèle de filtrage`.

En effet, ces options vont orienter l'architecture de vos réseaux internes ainsi qu'une partie importante de la politique de sécurité qui sera mise en place.

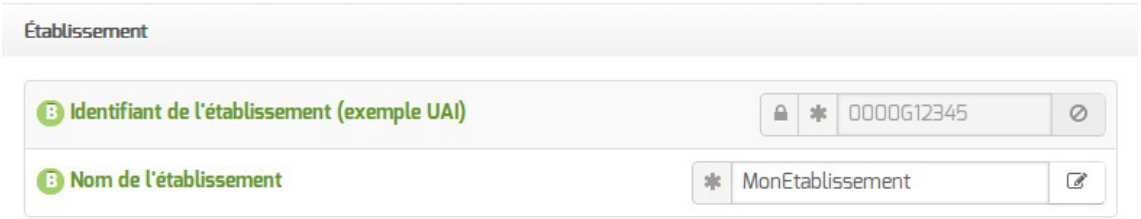
Le nombre d'interfaces doit, bien évidemment, être choisi en fonction du nombre de cartes réseau physiques du serveur mais plus encore en fonction du nombre de sous-réseaux souhaités.

Le modèle de filtrage doit être choisi en fonction du nombre d'interfaces activées et des services que l'on souhaite mettre en place.

1.1. Onglet Général

Présentation des différents paramètres de l'onglet `Général`.

Informations sur l'établissement



Deux informations sont importantes pour l'établissement :

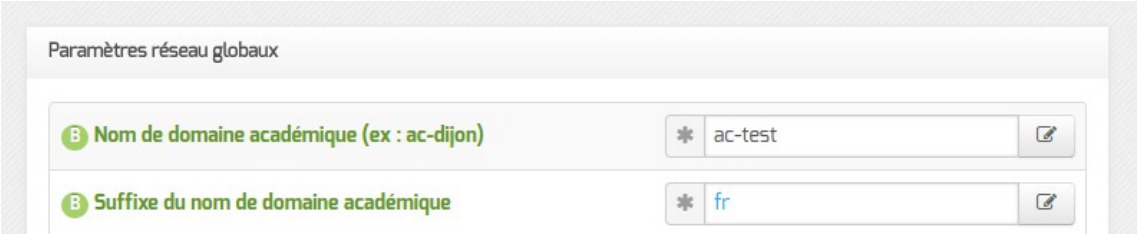
- l'`Identifiant de l'établissement`, qui doit être unique ;
- le `Nom de l'établissement`.

Ces informations sont notamment utiles pour Zéphir, les applications web locales, ...

Sur les modules fournissant un annuaire LDAP[p.307] local, ces variables sont utilisées pour créer l'arborescence.

Il est déconseillé de modifier ces informations après l'instanciation du serveur sur les modules utilisant un serveur LDAP local.

Paramètres réseau globaux



En premier lieu, il convient de configurer les noms de domaine de la machine.

Cette information est découpée en plusieurs champs :

- le nom de la machine dans l'établissement ;
- le nom du domaine privé utilisé à l'intérieur de l'établissement ;
- le nom de domaine académique et son suffixe.

Le `Nom de la machine` est laissé à l'appréciation de l'administrateur.

Les domaines de premier niveau `.com`, `.fr` sont en vigueur sur Internet, mais sont le résultat d'un choix arbitraire.

Sur un réseau local les noms de domaine sont privés et on peut tout à fait utiliser des domaines de premier niveau, et leur donner la sémantique que l'on veut.

Le `Nom de domaine privé du réseau local` utilise fréquemment des domaines de premier niveau du type `.lan` ou `.local`.

C'est ce nom qui configurera le serveur DNS (sur un module Amon par exemple) comme zone de résolution par défaut. Il sera utilisé par les machines pour résoudre l'ensemble des adresses locales.

Les informations sur les noms de domaine sont importantes car elles sont notamment utilisées pour l'envoi des courriels et pour la création de l'arborescence de l'annuaire LDAP.

L'usage d'un domaine de premier niveau utilisé sur Internet n'est pas recommandé, car il existe un risque de collision entre le domaine privé et le domaine public.

Nombre d'interfaces

Un module Amon peut avoir de 2 à 5 cartes réseau.

Le nombre d'interfaces activées se définit dans l'onglet `Général` de l'interface de configuration du module.

Cela ajoute autant d'onglets `Interface-n` que le nombre d'interfaces à activer choisi.

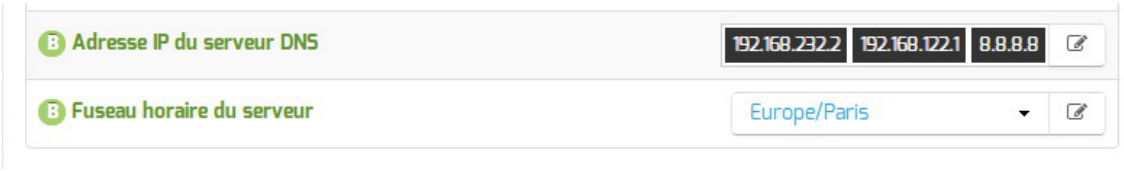
Proxy

Si le module doit utiliser un proxy pour accéder à Internet, il faut activer cette fonctionnalité en passant la variable `Utiliser un serveur mandataire (proxy) pour accéder à Internet` à `oui`.

Il devient alors possible de saisir la configuration du serveur proxy :

- nom de domaine ou adresse IP du serveur proxy ;
- le port du proxy.

DNS et fuseau horaire



La variable `Adresse IP du serveur DNS` donne la possibilité de saisir une ou plusieurs adresses IP du ou des serveur(s) de noms DNS[p.304].

La variable `Fuseau horaire du serveur` vous permet de choisir votre fuseau horaire dans une liste conséquente de propositions.

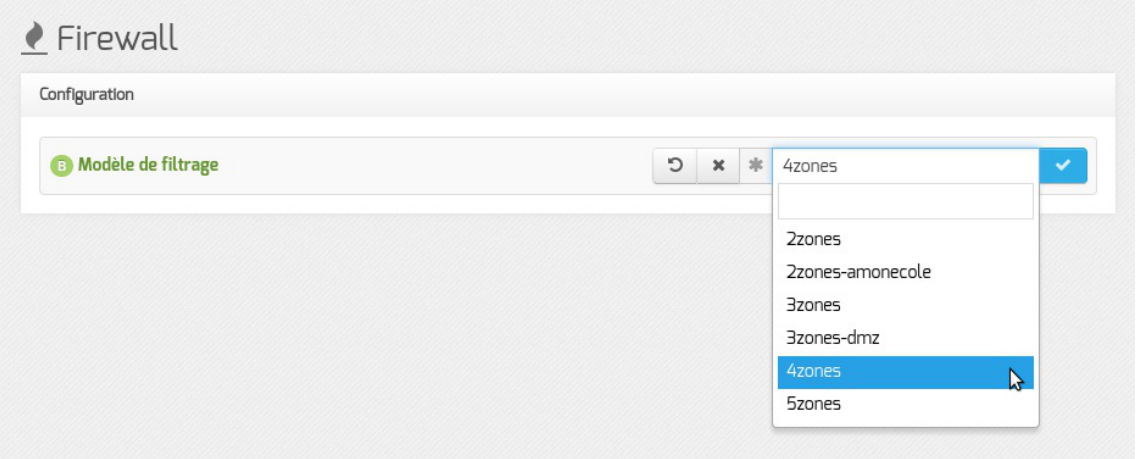
Voir aussi...

Onglet Interface-n [p.27]

1.2. Onglet Firewall

Modèle de filtrage

Le modèle de filtrage doit être choisi en fonction du nombre d'interfaces activées et des services que l'on souhaite mettre en place.



Par convention le premier caractère des modèles de filtrage proposés est un chiffre qui correspond au nombre d'interfaces désirées.

Les modèles de zone par défaut proposés supportent jusqu'à 5 cartes réseau :

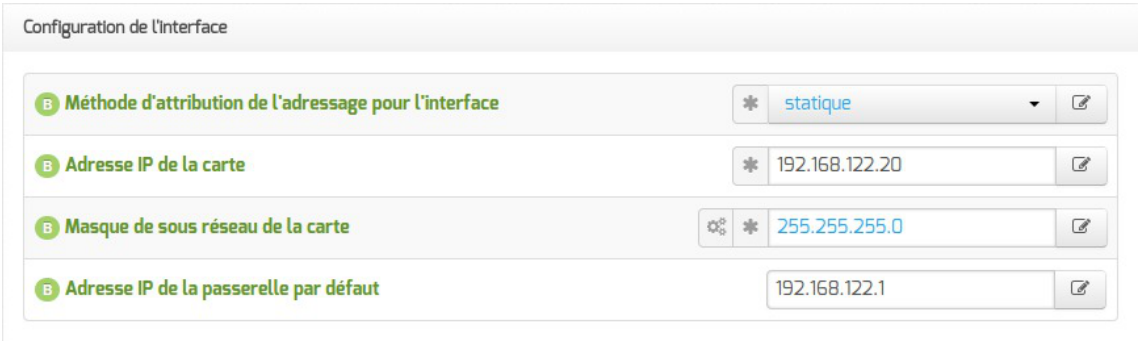
- **2zones** : gestion d'une zone admin ou pedago sur eth1 ;
- **2zones-amonecole** : modèle spécifique au module AmonEcole (pedago sur eth1) ;
- **3zones** : gestion d'une zone admin sur eth1 et d'une zone pedago sur eth2 ;
- **3zones-dmz** : gestion d'une zone pedago sur eth1 et d'une zone DMZ publique pouvant accueillir un module Scribe sur eth2 ;
- **4zones** : gestion d'une zone admin sur eth1, d'une zone pedago sur eth2 et d'une zone DMZ publique pouvant accueillir un module Scribe sur eth3 ;
- **5zones** : gestion d'une zone admin sur eth1, d'une zone pedago sur eth2, d'une zone DMZ publique pouvant accueillir un module Scribe sur eth3 et d'une zone DMZ privée sur eth4.

Le modèle de zone proposés correspondent à un modèle de filtrage ERA. Les modèles de filtrage ERA sont la description de pare-feu enregistrés dans des fichiers XML situés par défaut dans le répertoire `/usr/share/era/modeles/`.

Avec ERA il est possible de créer un nouveau modèle personnalisé dans le répertoire `/usr/share/era/modeles/`. Celui-ci apparaîtra dans la liste des modèles proposés par défaut.

1.3. Onglet Interface-0

Configuration de l'interface



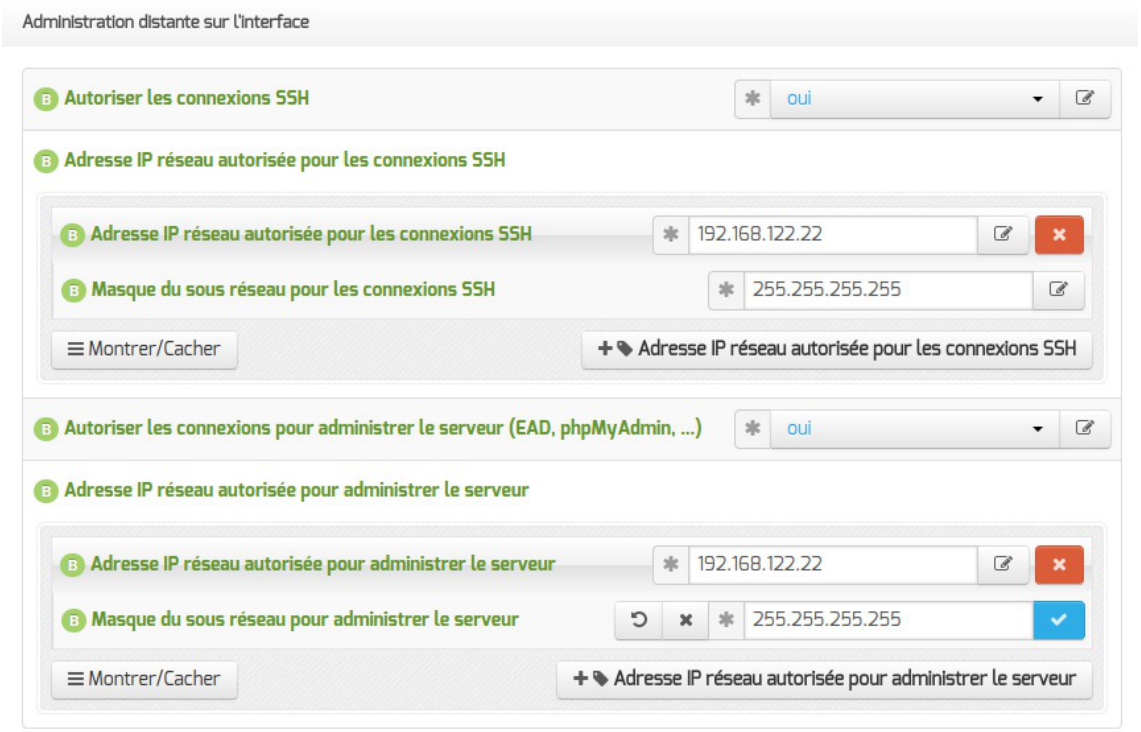
Configuration de l'interface

Avant toute chose, il faut savoir comment la carte réseau est configurée. Pour cela, il existe trois possibilités : statique, DHCP[p.303] et PPPoE[p.311].

- Dans le cas de la configuration statique, il faut renseigner l'adresse IP, le masque et la passerelle.
- La configuration DHCP ne nécessite aucun paramétrage particulier.
- En mode PPPoE, l'identifiant et le mot de passe de la connexion sont à renseigner.

EOLE est pleinement fonctionnel avec une connexion en IP fixe. Si vous ne disposez pas d'IP fixe, certaines fonctionnalités ne seront plus disponibles.

Administration à distance



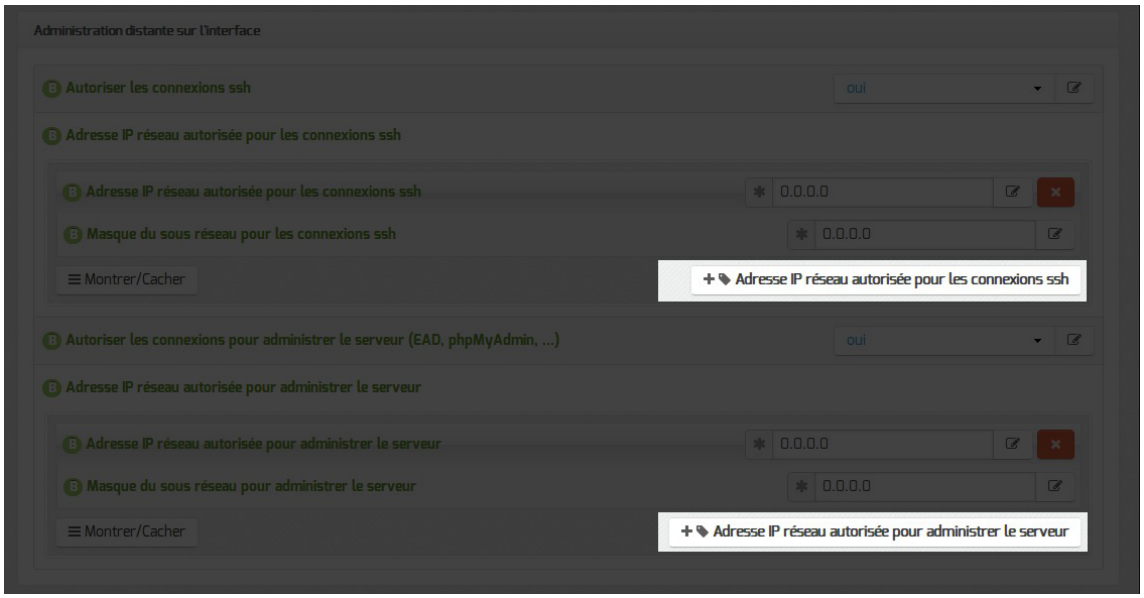
Configuration de l'administration à distance sur une interface

Par défaut les accès SSH[p.313] et aux différentes interfaces d'administration (EAD, phpMyAdmin, CUPS, ARV... selon le module) sont bloqués.

Pour chaque interface réseau activée (onglets `Interface-n`), il est possible d'autoriser des adresses IP

ou des adresses réseau à se connecter.

Les adresses autorisées à se connecter via SSH sont indépendantes de celles configurées pour accéder aux interfaces d'administration.



Il est possible d'autoriser plusieurs adresses en cliquant sur `Adresse IP réseau autorisée pour…`.

Le masque réseau d'une station isolée est `255.255.255.255`.

Dans le cadre de test sur un module l'utilisation de la valeur `0.0.0.0` dans les champs `Adresse IP réseau autorisée pour les connexions SSH` et `Masque du sous réseau pour les connexions SSH` autorise les connexions SSH depuis n'importe quelle adresse IP.

La commande suivante permet d'observer les connexions SSH arrivant sur un serveur EOLE : `tcpdump -nni $(CreoleGet nom_carte_eth0) port 22`

Des restrictions supplémentaires au niveau des connexions SSH sont disponibles dans l'onglet `Sshd` en mode expert.

1.4. Onglet Interface-1

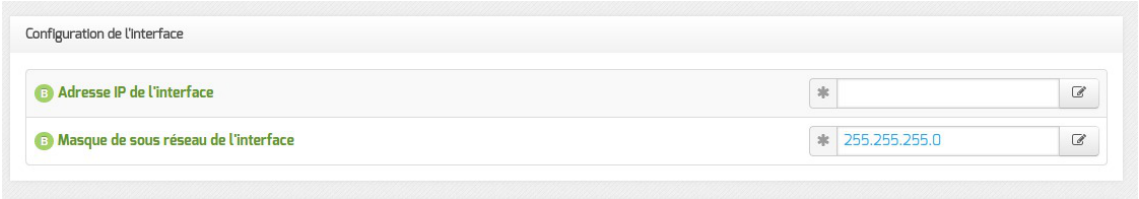
Nombre d'interfaces

Un module Amon peut avoir de 2 à 5 cartes réseau.

Le nombre d'interfaces activées se définit dans l'onglet `Général` de l'interface de configuration du module.

Cela ajoute autant d'onglets `Interface-n` que le nombre d'interfaces à activer choisi.

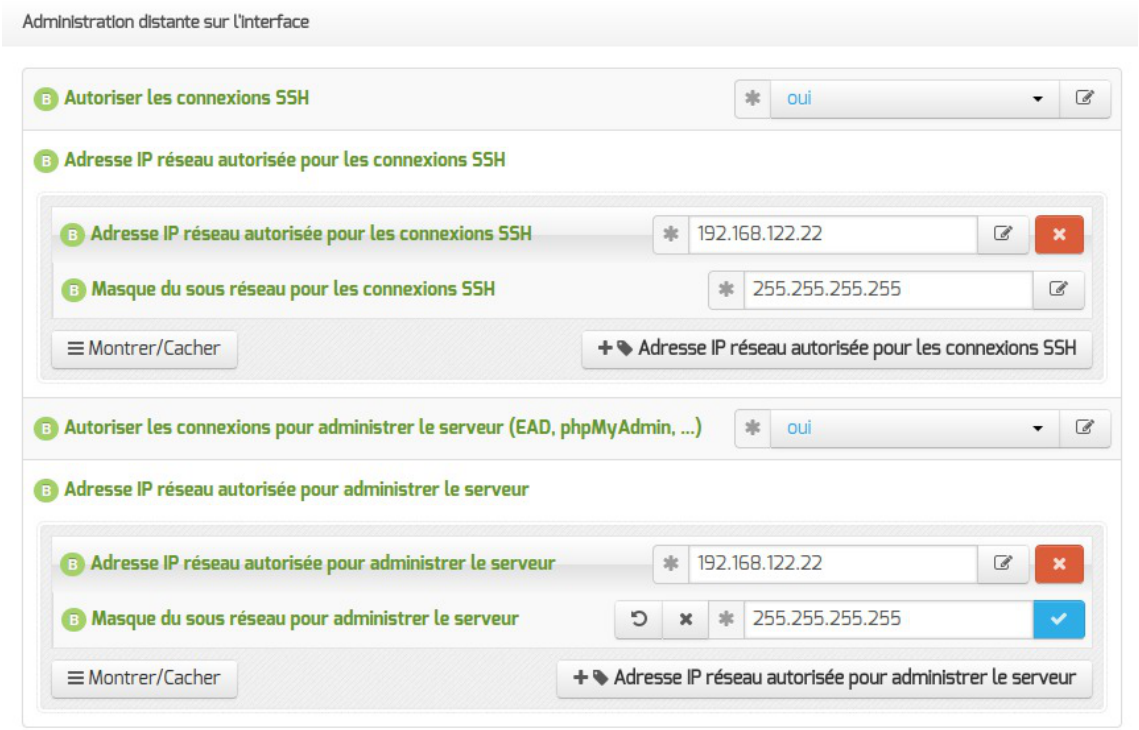
Configuration de l'interface



Configuration de l'interface

L'interface réseau nécessite un adressage statique, il faut renseigner l'adresse IP et le masque.

Administration à distance

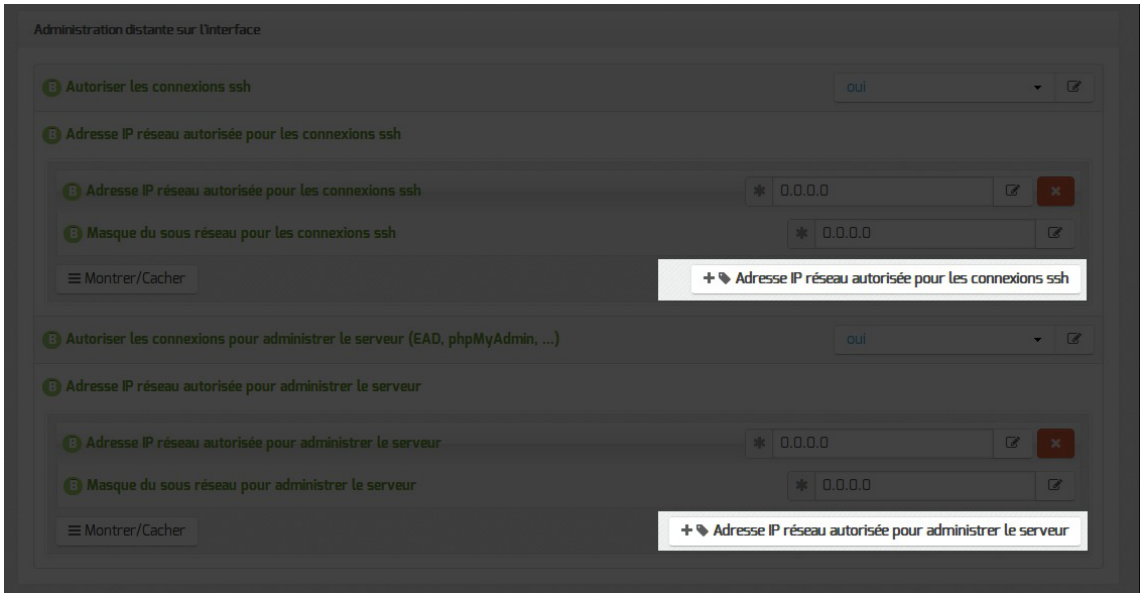


Configuration de l'administration à distance sur une interface

Par défaut les accès SSH[p.313] et aux différentes interfaces d'administration (EAD, phpMyAdmin, CUPS, ARV... selon le module) sont bloqués.

Pour chaque interface réseau activée (onglets `Interface-n`), il est possible d'autoriser des adresses IP ou des adresses réseau à se connecter.

Les adresses autorisées à se connecter via SSH sont indépendantes de celles configurées pour accéder aux interfaces d'administration.



Il est possible d'autoriser plusieurs adresses en cliquant sur `Adresse IP réseau autorisée pour…`.

Le masque réseau d'une station isolée est `255.255.255.255`.

Dans le cadre de test sur un module l'utilisation de la valeur `0.0.0.0` dans les champs `Adresse IP réseau autorisée pour les connexions SSH` et `Masque du sous réseau pour les connexions SSH` autorise les connexions SSH depuis n'importe quelle adresse IP.

La commande suivante permet d'observer les connexions SSH arrivant sur un serveur EOLE : `tcpdump -nni $(CreoleGet nom_carte_eth0) port 22`

Des restrictions supplémentaires au niveau des connexions SSH sont disponibles dans l'onglet `Sshd` en mode expert.

1.5. Onglet Interface-n

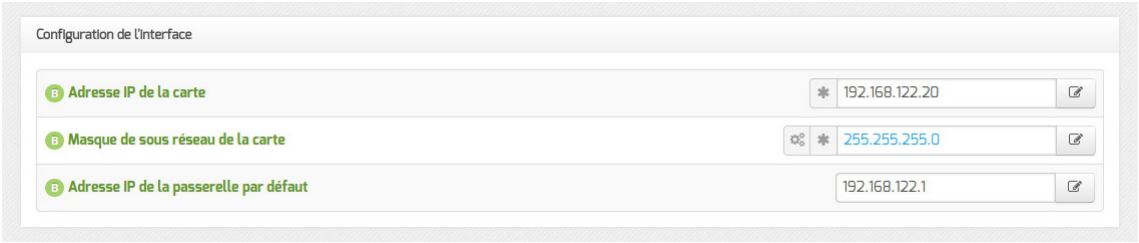
Nombre d'interfaces

Un module Amon peut avoir de 2 à 5 cartes réseau.

Le nombre d'interfaces activées se définit dans l'onglet `Général` de l'interface de configuration du module.

Cela ajoute autant d'onglets `Interface-n` que le nombre d'interfaces à activer choisi.

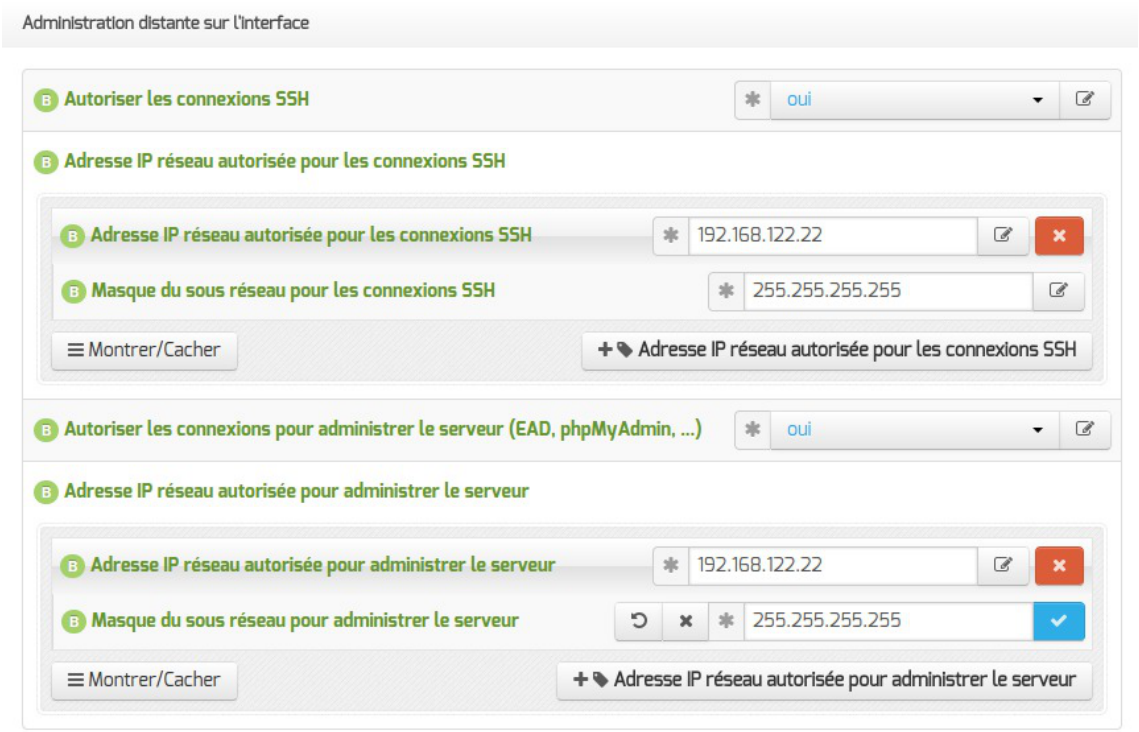
Configuration de l'interface



Configuration de l'interface

L'interface 0 nécessite un adressage statique, il faut renseigner l'adresse IP, le masque et la passerelle.

Administration à distance

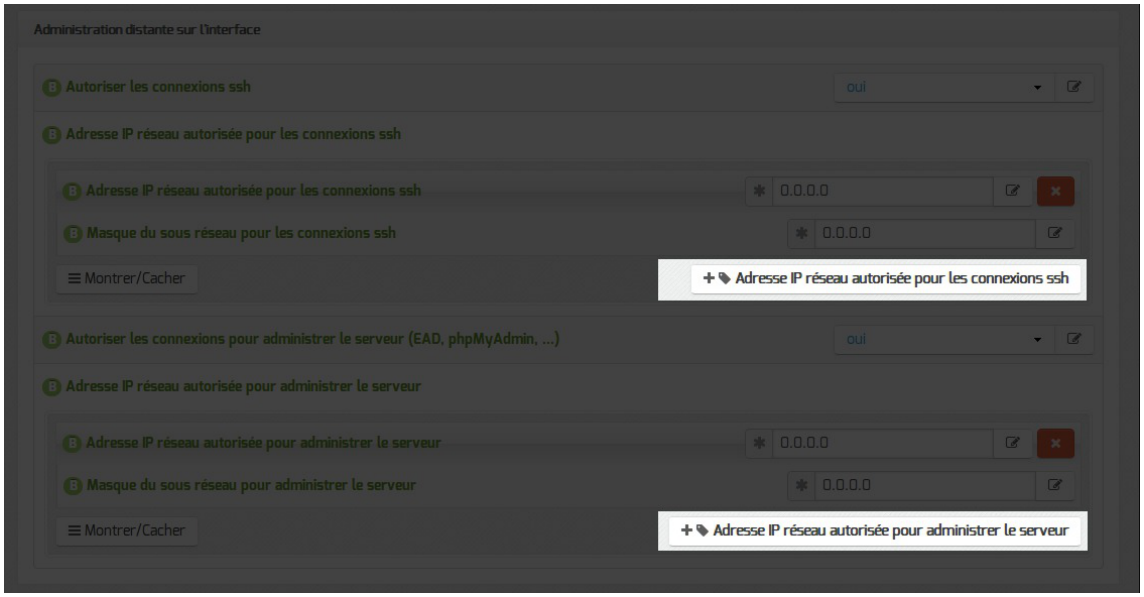


Configuration de l'administration à distance sur une interface

Par défaut les accès SSH[p.313] et aux différentes interfaces d'administration (EAD, phpMyAdmin, CUPS, ARV... selon le module) sont bloqués.

Pour chaque interface réseau activée (onglets `Interface-n`), il est possible d'autoriser des adresses IP ou des adresses réseau à se connecter.

Les adresses autorisées à se connecter via SSH sont indépendantes de celles configurées pour accéder aux interfaces d'administration.



Il est possible d'autoriser plusieurs adresses en cliquant sur `Adresse IP réseau autorisée pour…`.

Le masque réseau d'une station isolée est `255.255.255.255`.

Dans le cadre de test sur un module l'utilisation de la valeur `0.0.0.0` dans les champs `Adresse IP réseau autorisée pour les connexions SSH` et `Masque du sous réseau pour les connexions SSH` autorise les connexions SSH depuis n'importe quelle adresse IP.

Des restrictions supplémentaires au niveau des connexions SSH sont disponibles dans l'onglet `Sshd` en mode expert.

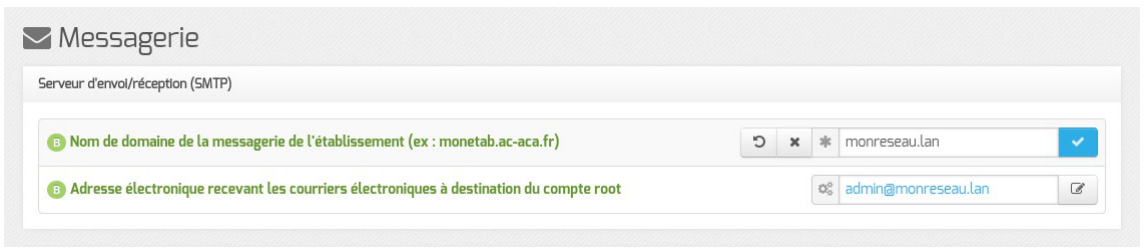
1.6. Onglet Messagerie

Même sur les modules ne fournissant aucun service directement lié à la messagerie, il est nécessaire de configurer une passerelle SMTP valide car de nombreux outils sont susceptibles de nécessiter l'envoi de mails.

La plupart des besoins concernent l'envoi d'alertes ou de rapports.

Exemples : rapports de sauvegarde, alertes système, ...

Serveur d'envoi/réception



Les paramètres communs à renseigner sont les suivants :

- `Nom de domaine de la messagerie de l'établissement (ex : monetab.ac-aca.fr)`, saisir un nom de domaine valide, par défaut un domaine privé est automatiquement créé avec le préfixe `i-`;
- `Adresse électronique recevant les courriers électroniques à destination du compte root`, permet de configurer une adresse pour recevoir les éventuels messages envoyés par le système.

Le `Nom de domaine de la messagerie de l'établissement` (onglet `Messagerie`) ne peut pas être le même que celui d'un conteneur. Le nom de la machine (onglet `Général`) donne son nom au conteneur maître aussi le `Nom de domaine de la messagerie de l'établissement` ne peut pas avoir la même valeur.

Dans le cas contraire les courriers électroniques utilisant le nom de domaine de la messagerie de l'établissement seront réécris et envoyés à l'adresse électronique d'envoi du compte root.

Cette contrainte permet de faire en sorte que les courrier électroniques utilisant un domaine de type `@<NOM CONTENEUR>.*` soit considéré comme des courriers électroniques systèmes.

Relai des messages

La variable `Passerelle SMTP`, permet de saisir l'adresse IP ou le nom DNS de la passerelle SMTP à utiliser.

Afin d'envoyer directement des courriers électroniques sur Internet il est possible de désactiver l'utilisation d'une passerelle en passant `Router les courriels par une passerelle SMTP` à `non`.

Sur les modules possédant un serveur SMTP (Scribe, AmonEcole), ces paramètres sont légèrement différents et des services supplémentaires sont configurables.

1.7. Onglet Proxy authentifié : 5 méthodes d'authentification

EOLE propose un mécanisme d'authentification web via un proxy.

Tous les accès web (HTTP et HTTPS) nécessiteront alors une phase d'authentification.

Cette fonctionnalité offre deux avantages :

- il sera possible de savoir quel utilisateur a accédé à une ressource particulière ;
- il sera possible d'appliquer des politiques de filtrage pour chaque utilisateur.

Pour profiter de cette fonctionnalité, il faut activer l'authentification du proxy dans l'onglet Authentification : `Activer l'authentification web (proxy)`.

Cinq méthodes d'authentification sont alors disponibles dans l'onglet Proxy authentifié.

Authentification NTLM/SMB

Il s'agit d'une authentification transparente pour les postes utilisateurs Windows intégrés dans un domaine Samba.

Il est possible de configurer plusieurs contrôleurs de domaine dans le cadre de l'authentification NTLM/SMB.

C'est la configuration à choisir si vous disposez d'un serveur pédagogique Scribe et/ou d'un serveur administratif Horus.

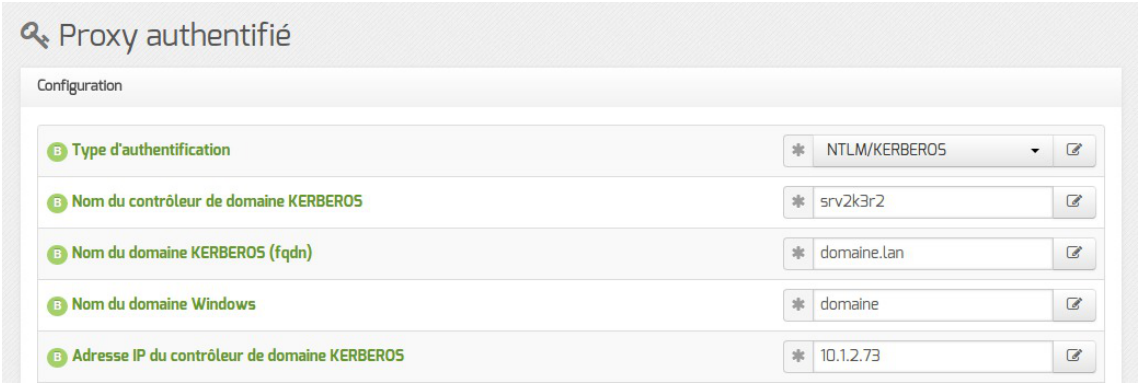
La syntaxe pour utiliser le proxy authentifié avec une machine hors domaine est `domaine\login` mais elle ne fonctionne pas avec toutes les versions de navigateurs.

L'authentification NTLM/SMB nécessite l'application de la clé de registre suivante sur les clients Windows Vista et Windows Seven :

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa]
"LMCompatibilityLevel"=dword:00000001
```

Pour plus d'informations, consulter : http://technet.microsoft.com/en-us/library/cc960646

Authentification NTLM/KERBEROS



Il s'agit d'une authentification transparente pour les postes utilisateurs Windows intégrés dans un domaine Active Directory.

Cette méthode d'authentification nécessite l'intégration du serveur au royaume Kerberos.

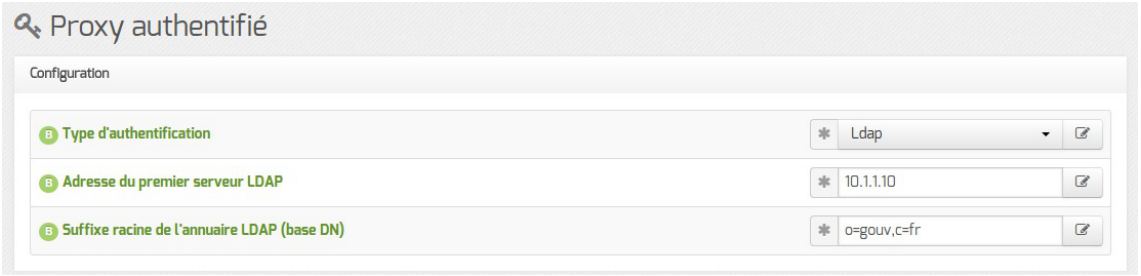
L'intégration peut être réalisée lors de l'instanciation du module en répondant `oui` à la question suivante :

```
Voulez-vous (ré)intégrer le serveur au domaine maintenant ?
```

Si la configuration de l'authentification NTLM/KERBEROS est réalisée après l'instanciation, il est possible de relancer l'intégration du serveur à tout moment à l'aide du script `enregistrement_domaine.sh`.

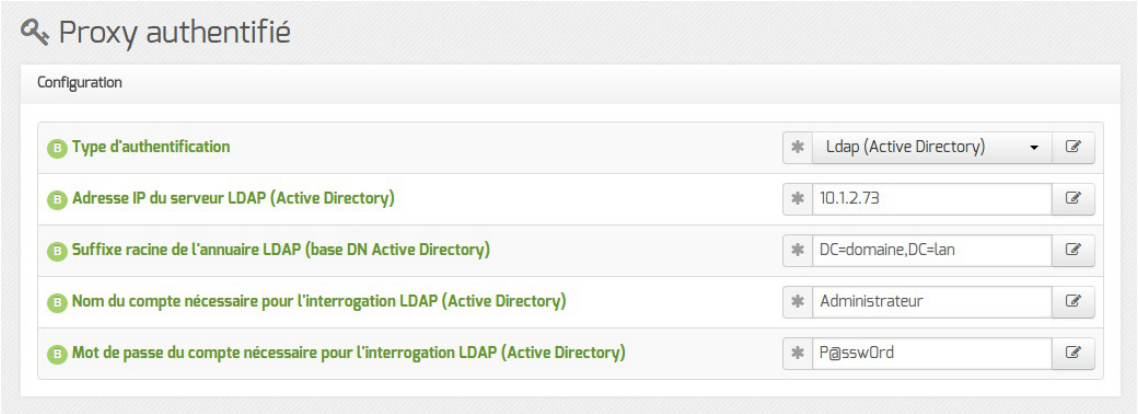
Authentification LDAP

Il s'agit d'une authentification non transparente s'appuyant sur un annuaire de type OpenLDAP.



Ce type d'authentification est recommandé pour les postes hors domaine.

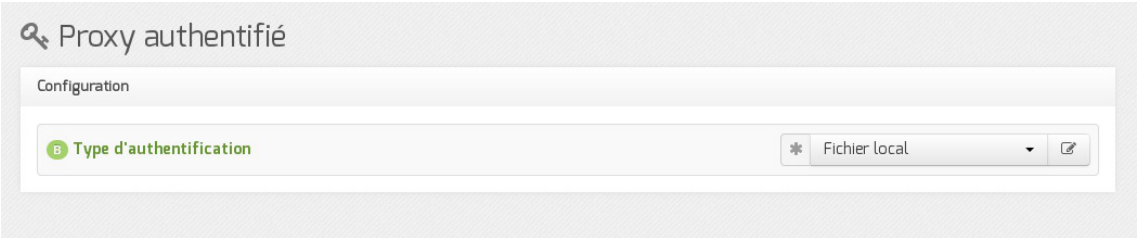
Authentification LDAP (Active Directory)



Il s'agit d'une authentification non transparente s'appuyant sur un annuaire de type Active Directory.

Ce type d'authentification est recommandé pour les postes hors domaine.

Authentification sur Fichier local



Il s'agit d'une authentification non transparente s'appuyant sur un fichier de comptes locaux.

Ce type d'authentification peut être utilisé dans une petite structure, comme une école, qui ne disposerait pas vraiment d'un réseau local.

Pour cette authentification, le fichier utilisé par défaut est : `/etc/squid3/users`

Il doit être au format *htpasswd* et il peut être peuplé en utilisant la commande suivante :

```
# htpasswd -c /etc/squid3/users <compte>
```

En mode conteneur (module AmonEcole par exemple), le fichier `/etc/squid3/users` se trouve dans le conteneur `proxy` :

```
# ssh proxy
# htpasswd -c /etc/squid3/users <compte>
```

ou

```
# CreoleRun "htpasswd -c /etc/squid3/users <compte>" proxy
```

Désactivation de l'authentification sur une interface

Pour chacune des interfaces (hors eth0 si plusieurs interfaces sont configurées), il est possible d'activer/désactiver l'authentification proxy.

Par exemple, pour désactiver l'authentification proxy uniquement sur le réseau eth2, il faut aller dans l'onglet `Interface-2` et répondre `non` à la question `Activer l'authentification sur cette`

`interface (s'applique aussi aux VLAN)`.

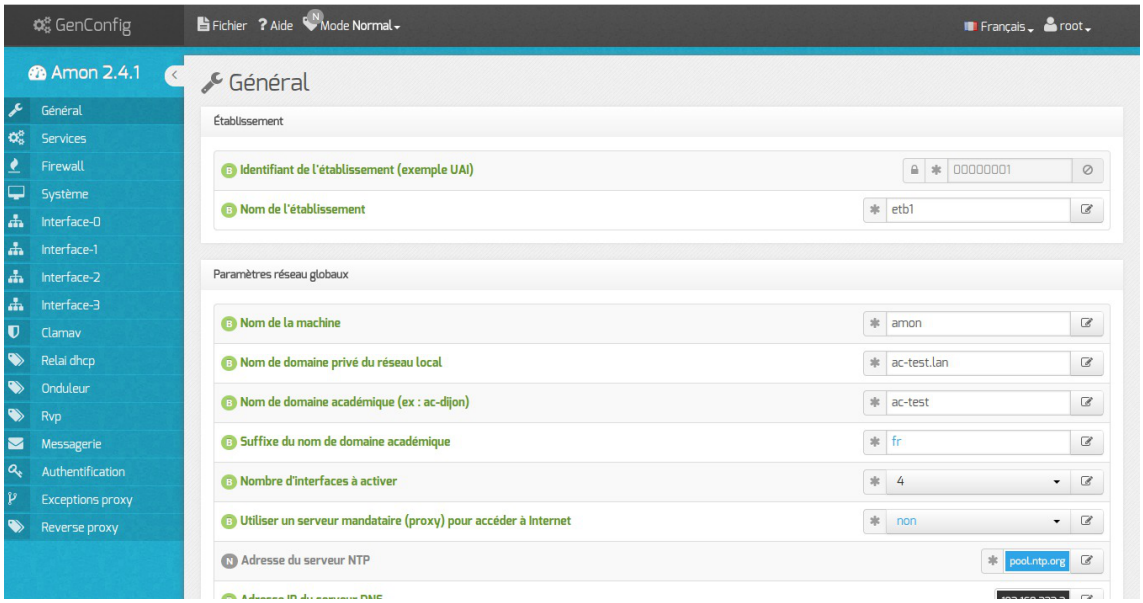
2. Configuration en mode normal

Certains onglets et certaines options ne sont disponibles qu'après avoir activé le mode normal de l'interface de configuration du module.

Dans l'interface de configuration du module voici les onglets propres à la configuration du module Amon :

- `Général` ;
- `Services` ;
- `Firewall` ;
- `Interface-0` (configuration de l'interface réseau) ;
- `Interface-1` (configuration de l'interface réseau) ;
- `Agregation` ** ;
- `Clamav` * ;
- `Relai dhcp` * ;
- `Onduleur` * ;
- `Rvp` * ;
- `Eole sso` * ;
- `Messagerie` ;
- `Authentification` ;
- `Proxy authentifié` ;
- `Proxy authentifié 2` ** ;
- `Wpad` ;
- `Exceptions proxy` ;
- `Reverse proxy` * ;
- `Freeradius`.

Certains des onglets ne sont disponibles qu'après activation du service dans l'onglet `Services` et sont marqués avec une * dans la liste ci-dessus.



Vue générale de l'interface de configuration du module

Dans les onglets `Général` et `Firewall`, deux options sont à renseigner avec la plus grande attention : le `Nombre d'interfaces à activer` et le `Modèle de filtrage`.

En effet, ces options vont orienter l'architecture de vos réseaux internes ainsi qu'une partie importante de la politique de sécurité qui sera mise en place.

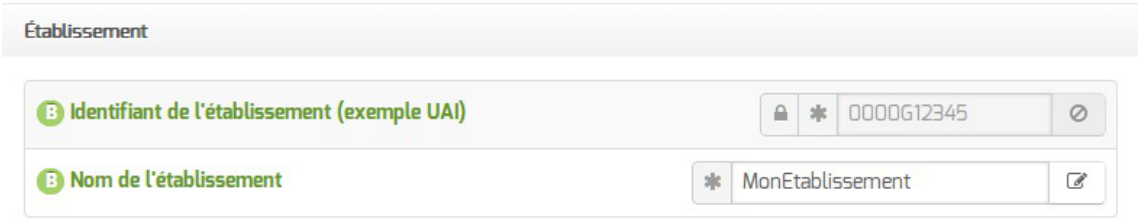
Le nombre d'interfaces doit, bien évidemment, être choisi en fonction du nombre de cartes réseau physiques du serveur mais plus encore en fonction du nombre de sous-réseaux souhaités.

Le modèle de filtrage doit être choisi en fonction du nombre d'interfaces activées et des services que l'on souhaite mettre en place.

2.1. Onglet Général

Présentation des différents paramètres de l'onglet `Général`.

Informations sur l'établissement

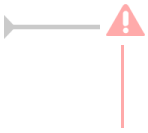


Deux informations sont importantes pour l'établissement :

- l'`Identifiant de l'établissement`, qui doit être unique ;
- le `Nom de l'établissement`.

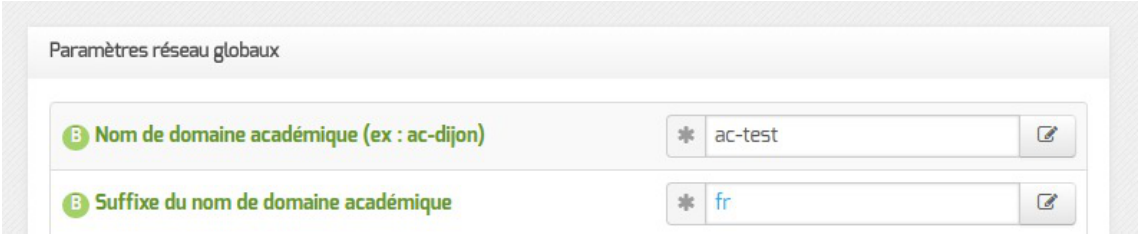
Ces informations sont notamment utiles pour Zéphir, les applications web locales, ...

Sur les modules fournissant un annuaire LDAP[p.307] local, ces variables sont utilisées pour créer l'arborescence.



Il est déconseillé de modifier ces informations après l'instanciation du serveur sur les modules utilisant un serveur LDAP local.

Paramètres réseau globaux



En premier lieu, il convient de configurer les noms de domaine de la machine.

Cette information est découpée en plusieurs champs :

- le nom de la machine dans l'établissement ;
- le nom du domaine privé utilisé à l'intérieur de l'établissement ;
- le nom de domaine académique et son suffixe.

Le `Nom de la machine` est laissé à l'appréciation de l'administrateur.

Les domaines de premier niveau `.com`, `.fr` sont en vigueur sur Internet, mais sont le résultat d'un choix arbitraire.

Sur un réseau local les noms de domaine sont privés et on peut tout à fait utiliser des domaines de premier niveau, et leur donner la sémantique que l'on veut.

Le `Nom de domaine privé du réseau local` utilise fréquemment des domaines de premier niveau du type `.lan` ou `.local`.

C'est ce nom qui configurera le serveur DNS (sur un module Amon par exemple) comme zone de résolution par défaut. Il sera utilisé par les machines pour résoudre l'ensemble des adresses locales.

Les informations sur les noms de domaine sont importantes car elles sont notamment utilisées pour l'envoi des courriels et pour la création de l'arborescence de l'annuaire LDAP.

L'usage d'un domaine de premier niveau utilisé sur Internet n'est pas recommandé, car il existe un risque de collision entre le domaine privé et le domaine public.

Nombre d'interfaces

Un module Amon peut avoir de 2 à 5 cartes réseau.

Le nombre d'interfaces activées se définit dans l'onglet `Général` de l'interface de configuration du module.

Cela ajoute autant d'onglets `Interface-n` que le nombre d'interfaces à activer choisi.

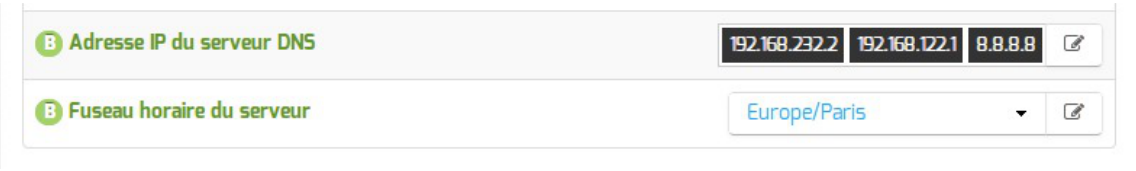
Proxy

Si le module doit utiliser un proxy pour accéder à Internet, il faut activer cette fonctionnalité en passant la variable `Utiliser un serveur mandataire (proxy) pour accéder à Internet` à `oui`.

Il devient alors possible de saisir la configuration du serveur proxy :

- nom de domaine ou adresse IP du serveur proxy ;
- le port du proxy.

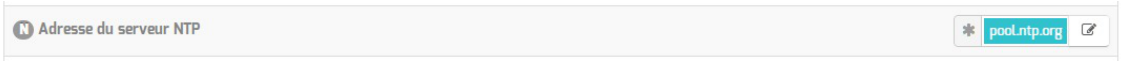
DNS et fuseau horaire



La variable `Adresse IP du serveur DNS` donne la possibilité de saisir une ou plusieurs adresses IP du ou des serveur(s) de noms DNS[p.304].

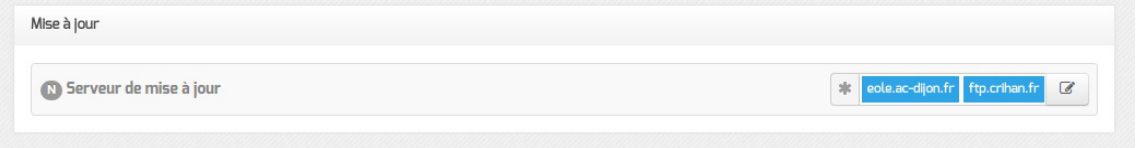
La variable `Fuseau horaire du serveur` vous permet de choisir votre fuseau horaire dans une liste conséquente de propositions.

NTP



Une valeur par défaut est attribuée pour le serveur de temps NTP[p.309]. Il est possible de changer cette valeur pour utiliser un serveur de temps personnalisé.

Mise à jour

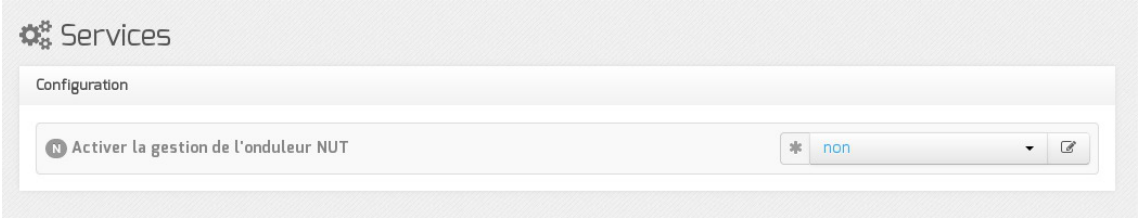


Il est possible de définir une autre adresse pour le serveur de mise à jour EOLE que celle fournie par défaut, dans le cas où vous auriez, par exemple, un miroir des dépôts.

Voir aussi...

- Onglet Interface-n [p.27]
- Les différentes mises à jour

2.2. Onglet Services



Vue de l'onglet Services en mode normal

Le service de base commun à tous les modules est la gestion de l'onduleur NUT[p.309].

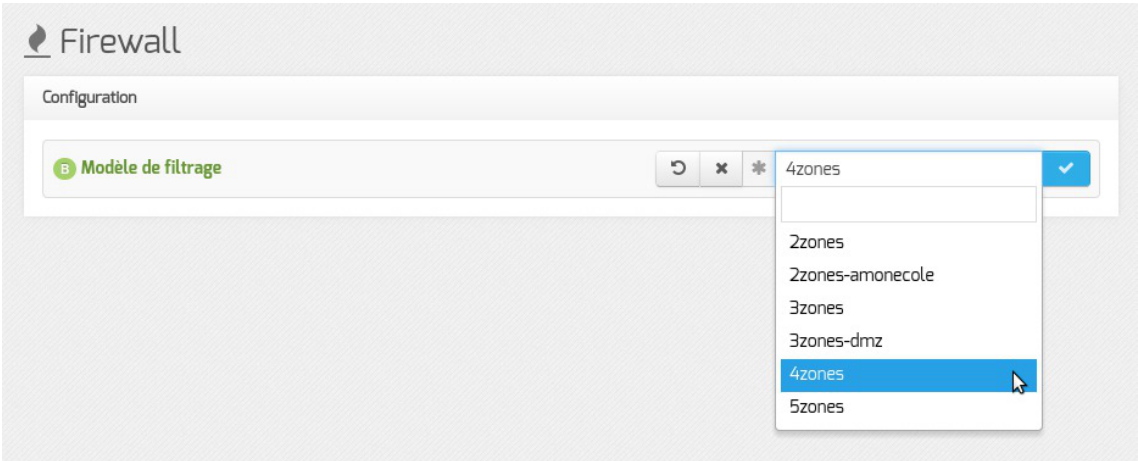
Les services de base propres au module Amon sont les suivants :

- l'anti-virus ClamAv ;
- le relai DHCP ;
- le réseau virtuel privé RVP ;
- le serveur EoleSSO ;
- le support WPAD ;
- le proxy inverse Nginx.

2.3. Onglet Firewall

Modèle de filtrage

Le modèle de filtrage doit être choisi en fonction du nombre d'interfaces activées et des services que l'on souhaite mettre en place.



Par convention le premier caractère des modèles de filtrage proposés est un chiffre qui correspond au nombre d'interfaces désirées.

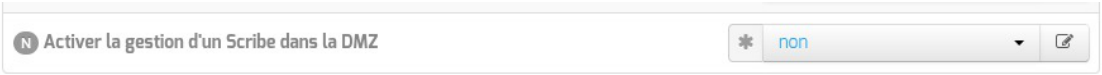
Les modèles de zone par défaut proposés supportent jusqu'à 5 cartes réseau :

- **2zones** : gestion d'une zone admin ou pedago sur eth1 ;
- **2zones-amonecole** : modèle spécifique au module AmonEcole (pedago sur eth1) ;
- **3zones** : gestion d'une zone admin sur eth1 et d'une zone pedago sur eth2 ;
- **3zones-dmz** : gestion d'une zone pedago sur eth1 et d'une zone DMZ publique pouvant accueillir un module Scribe sur eth2 ;
- **4zones** : gestion d'une zone admin sur eth1, d'une zone pedago sur eth2 et d'une zone DMZ publique pouvant accueillir un module Scribe sur eth3 ;
- **5zones** : gestion d'une zone admin sur eth1, d'une zone pedago sur eth2, d'une zone DMZ publique pouvant accueillir un module Scribe sur eth3 et d'une zone DMZ privée sur eth4.

Le modèle de zone proposés correspondent à un modèle de filtrage ERA. Les modèles de filtrage ERA sont la description de pare-feu enregistrés dans des fichiers XML situés par défaut dans le répertoire `/usr/share/era/modeles/`.

Avec ERA il est possible de créer un nouveau modèle personnalisé dans le répertoire `/usr/share/era/modeles/`. Celui-ci apparaîtra dans la liste des modèles proposés par défaut.

La variable `Activer la gestion d'un Scribe dans la DMZ` permet la prise en charge par bastion[p.302] des règles propres à la DMZ[p.304].



Si l'on souhaite mettre en place l'architecture suivante avec Amon :

- un réseau administratif ;
- un réseau pédagogique ;
- une DMZ contenant un serveur Scribe hébergeant des services web à ouvrir depuis l'extérieur.

La configuration recommandée sera :

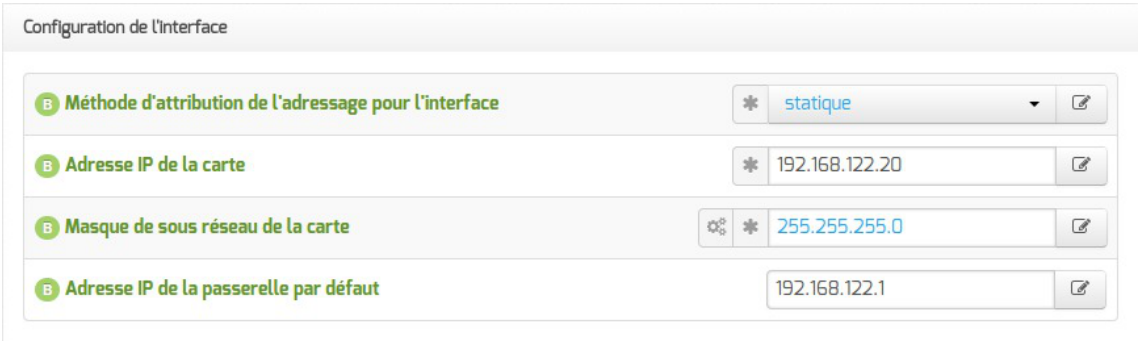
- `Nombre d'interfaces à activer` : `4` (onglet `Général` en mode basique) ;
- `Modèle de filtrage` : `4zones` (onglet `Firewall` en mode basique) ;
- `Activer la gestion d'un Scribe dans la DMZ` : `oui` (onglet `Firewall` en mode normal).

Voir aussi...

Configuration du module Amon avec le module Scribe en DMZ [p.187]

2.4. Onglet Interface-0

Configuration de l'interface



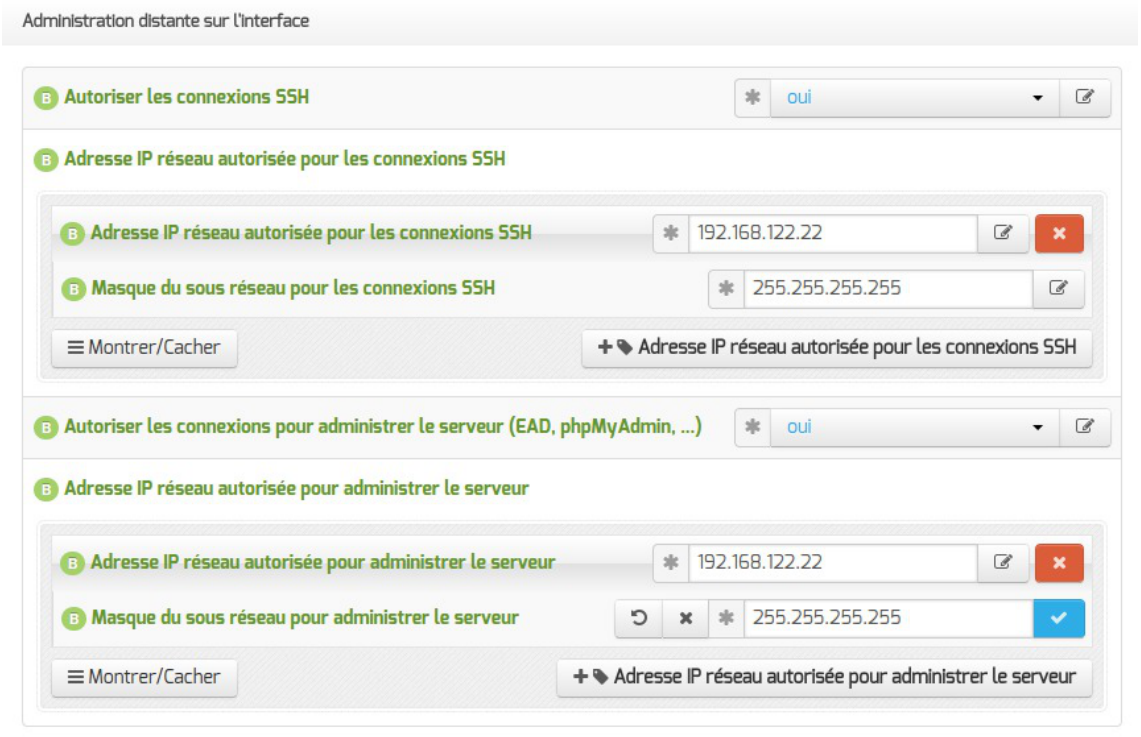
Configuration de l'interface

Avant toute chose, il faut savoir comment la carte réseau est configurée. Pour cela, il existe trois possibilités : statique, DHCP[p.303] et PPPoE[p.311].

- Dans le cas de la configuration statique, il faut renseigner l'adresse IP, le masque et la passerelle.
- La configuration DHCP ne nécessite aucun paramétrage particulier.
- En mode PPPoE, l'identifiant et le mot de passe de la connexion sont à renseigner.

> EOLE est pleinement fonctionnel avec une connexion en IP fixe. Si vous ne disposez pas d'IP fixe, certaines fonctionnalités ne seront plus disponibles.

Administration à distance

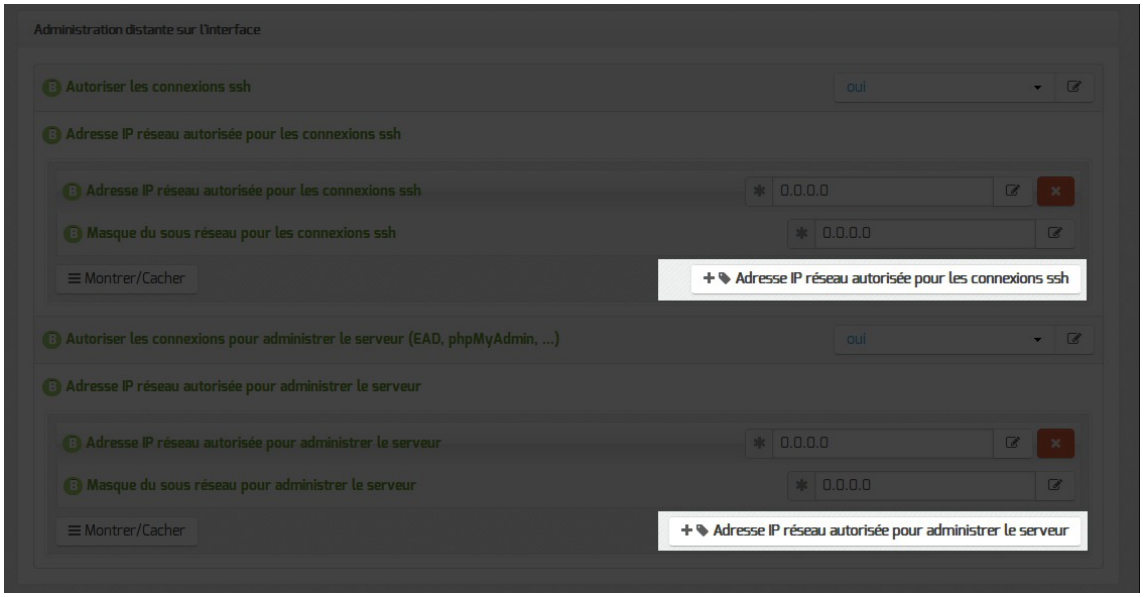


Configuration de l'administration à distance sur une interface

Par défaut les accès SSH[p.313] et aux différentes interfaces d'administration (EAD, phpMyAdmin, CUPS, ARV... selon le module) sont bloqués.

Pour chaque interface réseau activée (onglets `Interface-n`), il est possible d'autoriser des adresses IP ou des adresses réseau à se connecter.

Les adresses autorisées à se connecter via SSH sont indépendantes de celles configurées pour accéder aux interfaces d'administration.



Il est possible d'autoriser plusieurs adresses en cliquant sur `Adresse IP réseau autorisée pour…`.

Le masque réseau d'une station isolée est `255.255.255.255`.

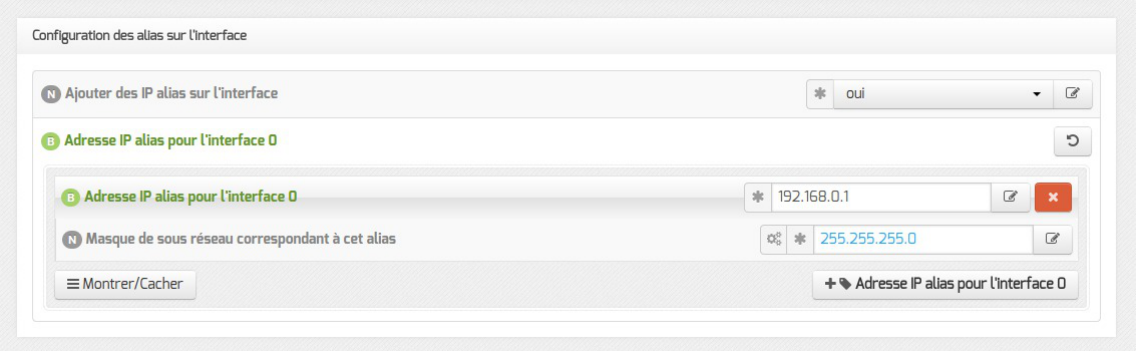
Dans le cadre de test sur un module l'utilisation de la valeur `0.0.0.0` dans les champs `Adresse IP réseau autorisée pour les connexions SSH` et `Masque du sous réseau pour les connexions SSH` autorise les connexions SSH depuis n'importe quelle adresse IP.

La commande suivante permet d'observer les connexions SSH arrivant sur un serveur EOLE : `tcpdump -nni $(CreoleGet nom_carte_eth0) port 22`

Des restrictions supplémentaires au niveau des connexions SSH sont disponibles dans l'onglet `Sshd` en mode expert.

Configuration des alias sur l'interface

EOLE supporte les alias sur les cartes réseau. Définir des alias IP consiste à affecter plus d'une adresse IP à une interface.

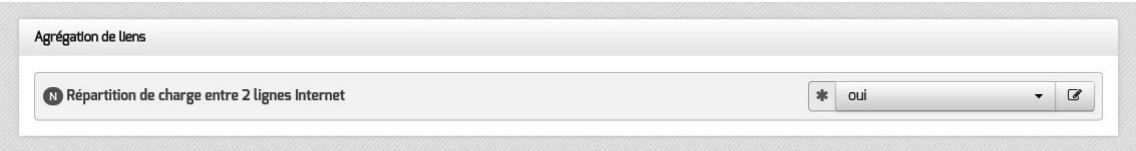


Pour cela, il faut activer son support (`Ajouter des IP alias sur l'interface` à `oui`) et configurer l'adresse IP et le masque de sous réseau.

Si l'agrégation de liens est activée. Il faut obligatoirement configurer une passerelle particulière pour cet alias.

Agrégation de liens

L'activation d'un alias IP, fait apparaître un nouveau paramètre, `Répartition de charge entre 2 lignes Internet`, qu'il faut passer à `oui`.



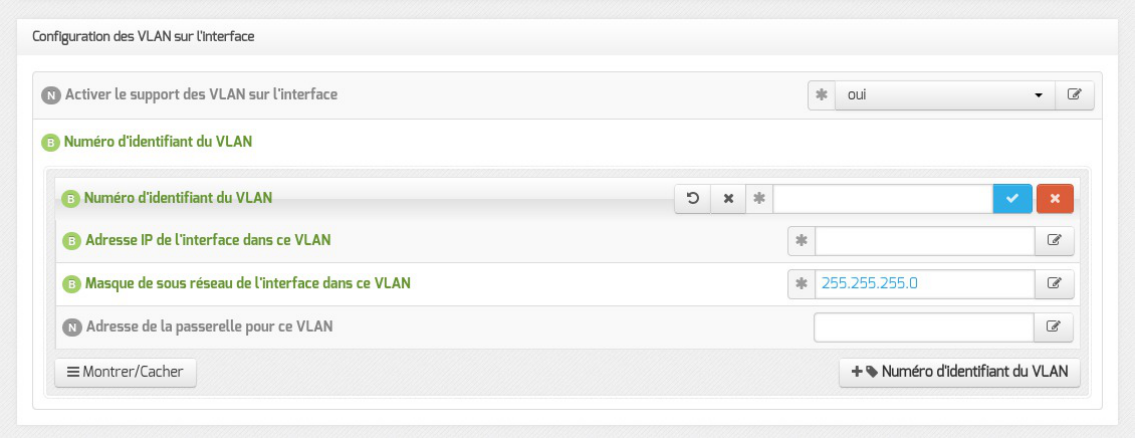
Activation de l'agrégation de lien

Un nouvel onglet, `Agrégation`, est disponible.

Si l'agrégation de liens est activée il faut obligatoirement configurer une passerelle particulière pour l'alias activé dans la rubrique `Configuration des alias sur l'interface`.

Configuration des VLAN sur l'interface

Il est possible de configurer des VLAN (réseau local virtuel) sur une interface déterminée du module.



Pour cela, il faut activer son support (`Activer le support des VLAN sur l'interface` à `oui` et ajout d'un numéro identifiant du VLAN avec le bouton `+ Numéro d'identifiant du VLAN`) et configurer l'ensemble des paramètres utiles (l'ID, l'adresse IP, ...).

Il est possible de configurer une passerelle particulière pour ce VLAN.

Voir aussi...

> Onglet Agrégation : Mise en place d'une répartition de charge ou d'une haute disponibilité [p.52]

2.5. Onglet Interface-1

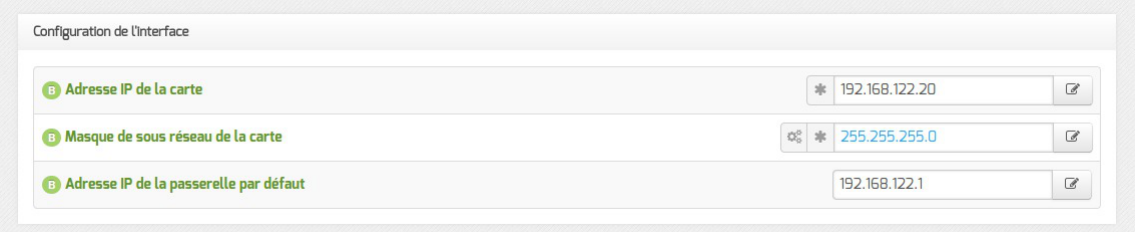
Nombre d'interfaces

Un module Amon peut avoir de 2 à 5 cartes réseau.

Le nombre d'interfaces activées se définit dans l'onglet `Général` de l'interface de configuration du module.

Cela ajoute autant d'onglets `Interface-n` que le nombre d'interfaces à activer choisi.

Configuration de l'interface



Configuration de l'interface

L'interface 0 nécessite un adressage statique, il faut renseigner l'adresse IP, le masque et la passerelle.

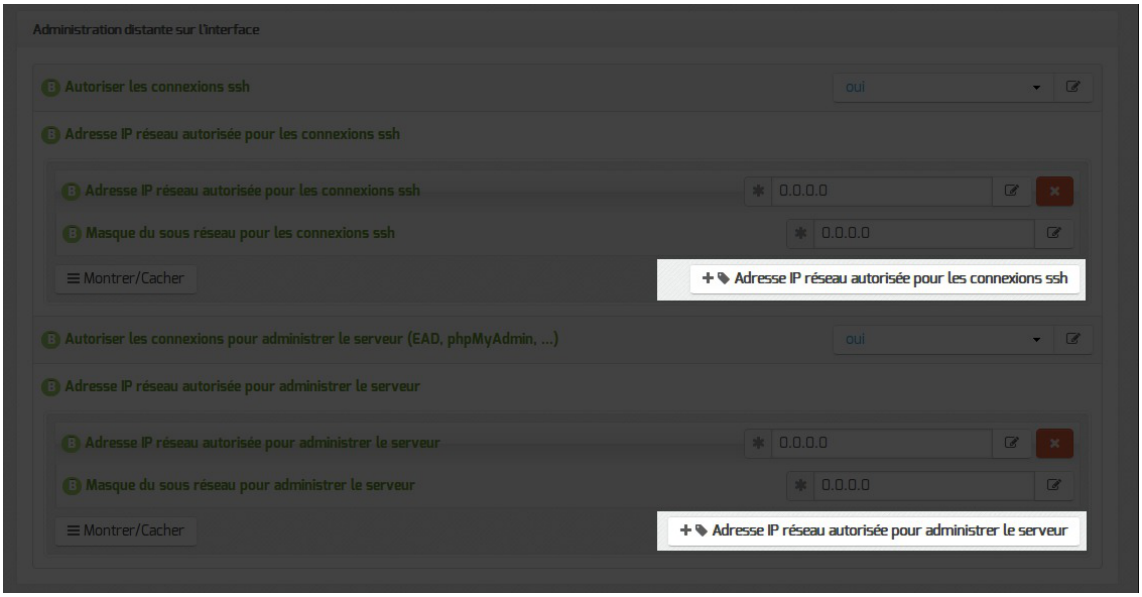
Administration à distance

Configuration de l'administration à distance sur une interface

Par défaut les accès SSH[p.313] et aux différentes interfaces d'administration (EAD, phpMyAdmin, CUPS, ARV... selon le module) sont bloqués.

Pour chaque interface réseau activée (onglets `Interface-n`), il est possible d'autoriser des adresses IP ou des adresses réseau à se connecter.

Les adresses autorisées à se connecter via SSH sont indépendantes de celles configurées pour accéder aux interfaces d'administration.



Il est possible d'autoriser plusieurs adresses en cliquant sur `Adresse IP réseau autorisée pour…`.

Le masque réseau d'une station isolée est `255.255.255.255`.

Dans le cadre de test sur un module l'utilisation de la valeur `0.0.0.0` dans les champs

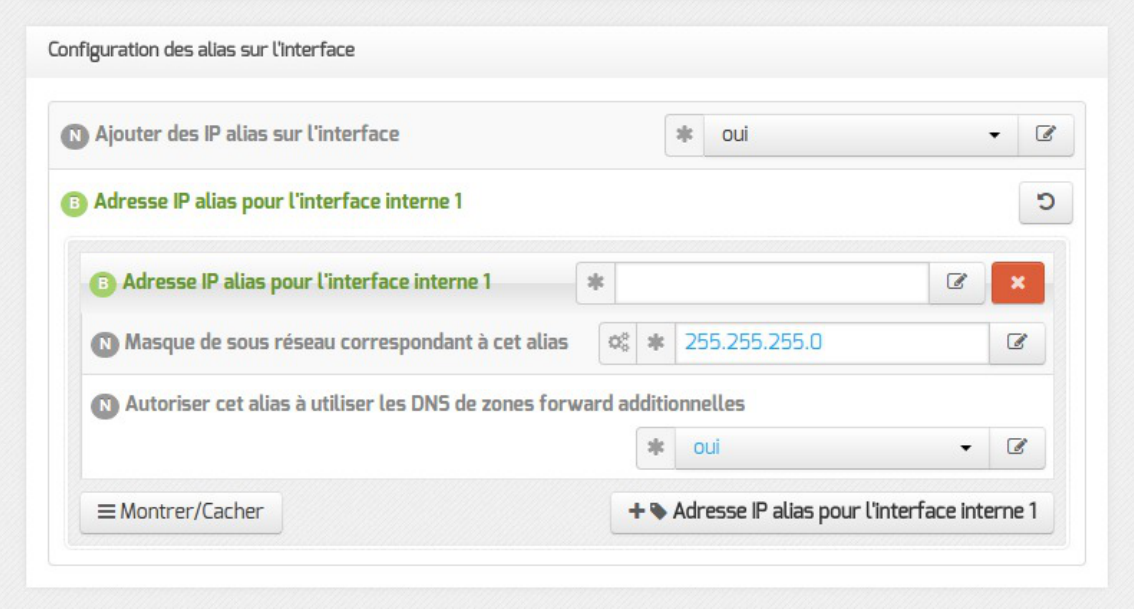
`Adresse IP réseau autorisée pour les connexions SSH` et `Masque du sous réseau pour les connexions SSH` autorise les connexions SSH depuis n'importe quelle adresse IP.

La commande suivante permet d'observer les connexions SSH arrivant sur un serveur EOLE : `tcpdump -nni $(CreoleGet nom_carte_eth0) port 22`

Des restrictions supplémentaires au niveau des connexions SSH sont disponibles dans l'onglet `Sshd` en mode expert.

Configuration des alias sur l'interface

EOLE supporte les alias sur les cartes réseau. Définir des alias IP consiste à affecter plus d'une adresse IP à une interface.



Pour cela, il faut activer son support (`Ajouter des IP alias sur l'interface` à `oui`) et configurer l'adresse IP et le masque de sous réseau.

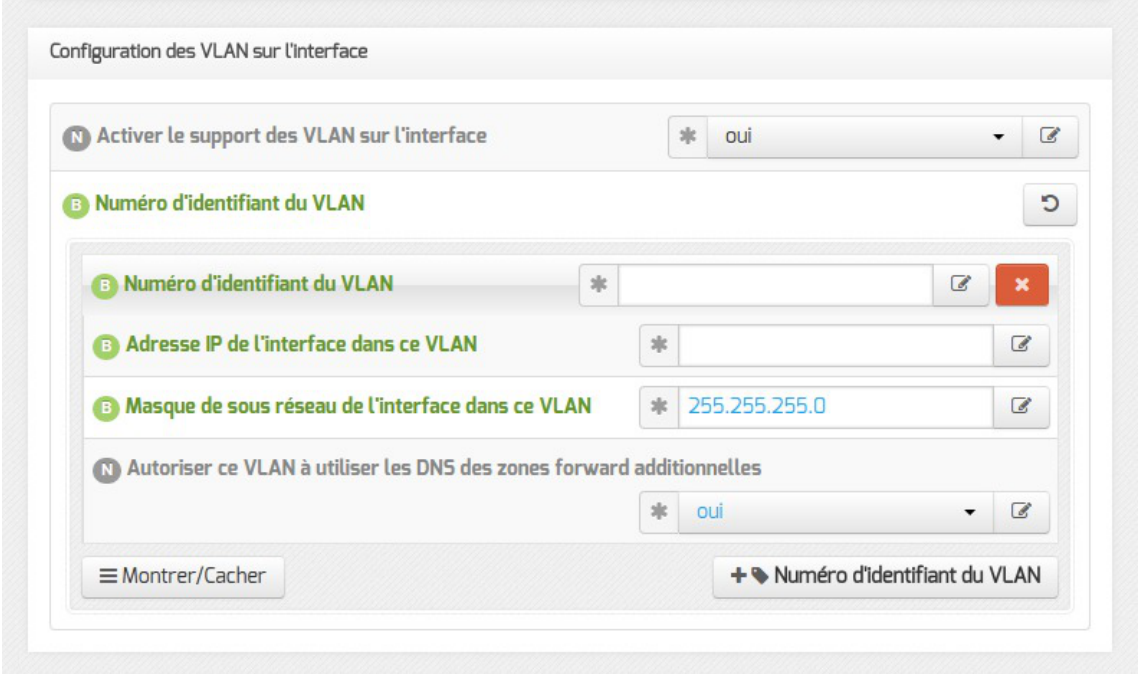
`Autoriser cet alias à utiliser les DNS de zones forward additionnelles` permet d'autoriser le réseau de cet alias à résoudre les noms d'hôte des domaines déclarés dans la section Forward de zone DNS de l'onglet `Zones-dns`.

Si le support du RVP est activé une option supplémentaire est disponible :

- `Autoriser cet alias à utiliser les DNS de Forward RVP/AGRIATES` : Si le service RVP est activé (onglet `Services`) et que le serveur est membre du réseau AGRIATES (onglet `Rvp`) la variable est disponible pour autoriser ou non cet alias à utiliser les DNS noms d'hôte de la zone AGRIATES.

Configuration des VLAN sur l'interface

Il est possible de configurer des VLAN (réseau local virtuel) sur une interface déterminée du module.



Pour cela, il faut activer son support (`Activer le support des VLAN sur l'interface` à `oui` et ajout d'un numéro identifiant du VLAN avec le bouton `+ Numéro d'identifiant du VLAN`) et configurer l'ensemble des paramètres utiles (l'ID, l'adresse IP, ...).

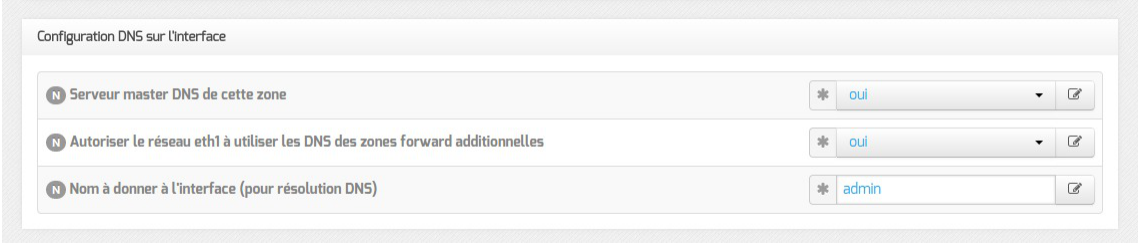
`Autoriser ce VLAN à utiliser les DNS des zones forward additionnelles` permet d'autoriser le réseau de ce VLAN à résoudre les noms d'hôte des domaines déclarés dans la section Forward de zone DNS de l'onglet `Zones-dns`.

Si le support du RVP est activé une option supplémentaire est disponible :

- `Autoriser ce VLAN à utiliser les DNS de Forward RVP/AGRIATES` : Si le service RVP est activé (onglet `Services`) et que le serveur est membre du réseau AGRIATES (onglet `Rvp`) la variable est disponible pour autoriser ou non ce VLAN à utiliser les DNS noms d'hôte de la zone AGRIATES.

Configuration DNS sur l'interface

Il est possible d'ajuster les paramètres du serveur DNS pour chaque interface réseau sauf pour l'interface 0.



- `Serveur master DNS de cette zone` : sert à activer le DNS sur l'interface.
- `Autoriser le réseau ethX à utiliser les DNS des zones forward`

`additionnels` : permet d'autoriser le réseau ethX à résoudre les noms d'hôte des domaines déclarés dans la section `Forward de zone DNS` de l'onglet `Zones-dns`.

- `Nom à donner à l'interface (pour résolution DNS)` : entrée DNS correspondant à l'adresse IP de l'interface ethX. Le nom par défaut (admin pour l'interface eth1) est différent et doit rester pour chaque interface.

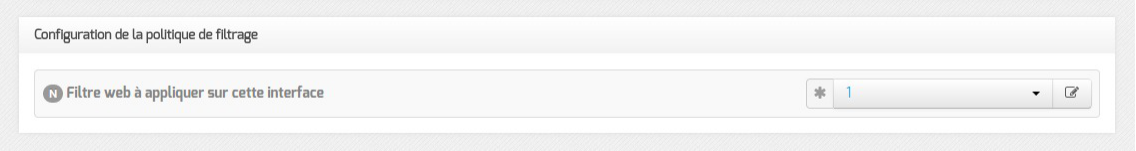
Si le support du RVP est activé une option supplémentaire est disponible :

- `Autoriser le réseau ethX à utiliser les DNS de forward RVP/AGRIATES` : Si le service RVP est activé (onglet `Services`) et que le serveur est membre du réseau AGRIATES (onglet `Rvp`) la variable est disponible pour autoriser ou non le réseau ethX à résoudre les noms d'hôte de la zone AGRIATES.

Configuration de la politique de filtrage

EOLE permet de différencier les zones suivant l'interface (administration ou pédagogie).

La différenciation se fait en modifiant la valeur choisie pour `Filtre Web à appliquer à cette interface` dans la configuration de chaque interface (onglets : `Interface-1`, `Interface-2`, ...).



Les filtres web 1 et 2 correspondent chacun à une instance du logiciel de filtrage. La configuration de chacun des filtres se fait dans l'onglet `Filtrage web`.

Voir aussi...

> Onglet Dansguardian : Configuration du filtrage web

2.6. Onglet Interface-n

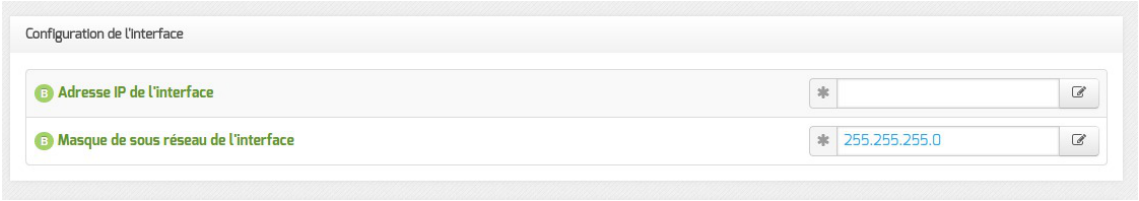
Nombre d'interfaces

Un module Amon peut avoir de 2 à 5 cartes réseau.

Le nombre d'interfaces activées se définit dans l'onglet `Général` de l'interface de configuration du module.

Cela ajoute autant d'onglets `Interface-n` que le nombre d'interfaces à activer choisi.

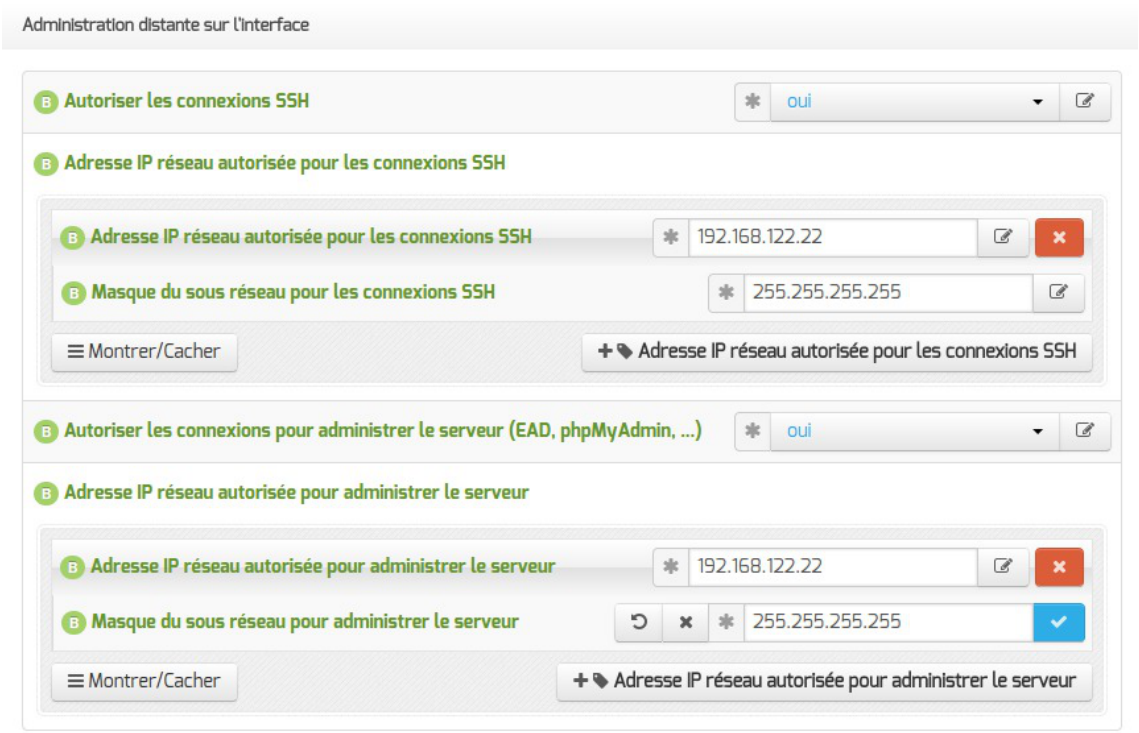
Configuration de l'interface



Configuration de l'interface

L'interface réseau nécessite un adressage statique, il faut renseigner l'adresse IP et le masque.

Administration à distance

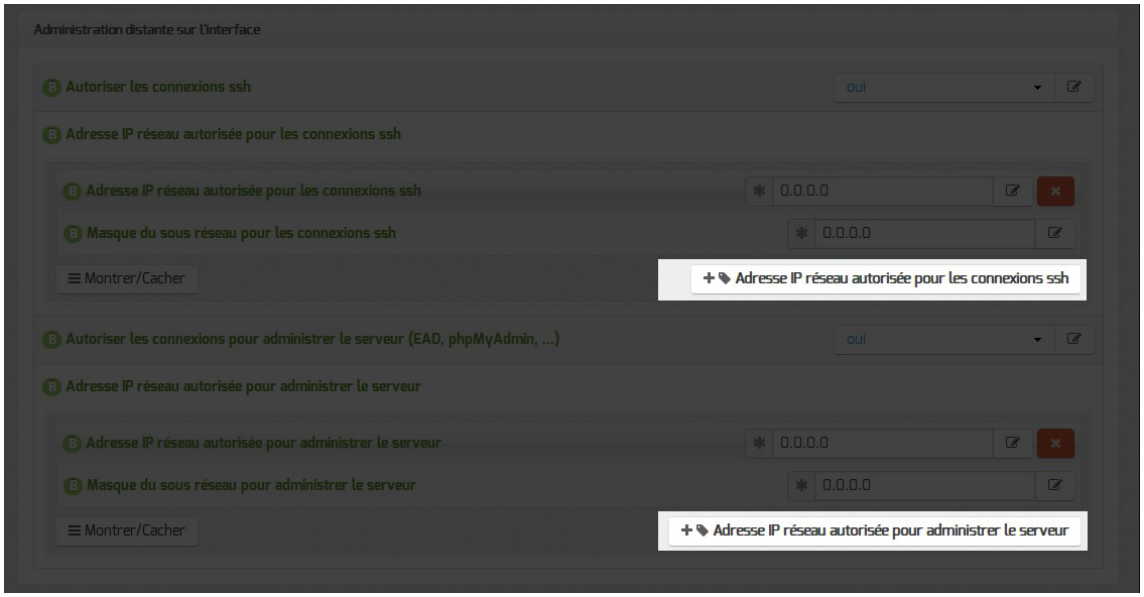


Configuration de l'administration à distance sur une interface

Par défaut les accès SSH[p.313] et aux différentes interfaces d'administration (EAD, phpMyAdmin, CUPS, ARV... selon le module) sont bloqués.

Pour chaque interface réseau activée (onglets `Interface-n`), il est possible d'autoriser des adresses IP ou des adresses réseau à se connecter.

Les adresses autorisées à se connecter via SSH sont indépendantes de celles configurées pour accéder aux interfaces d'administration.



Il est possible d'autoriser plusieurs adresses en cliquant sur `Adresse IP réseau autorisée pour…`.

Le masque réseau d'une station isolée est `255.255.255.255`.

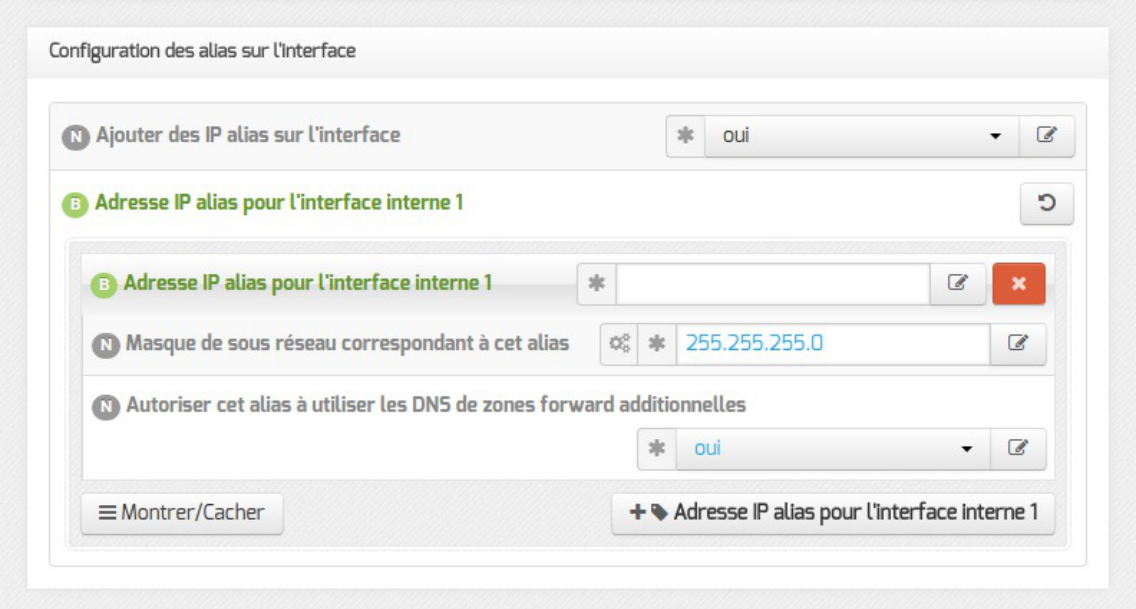
Dans le cadre de test sur un module l'utilisation de la valeur `0.0.0.0` dans les champs `Adresse IP réseau autorisée pour les connexions SSH` et `Masque du sous réseau pour les connexions SSH` autorise les connexions SSH depuis n'importe quelle adresse IP.

La commande suivante permet d'observer les connexions SSH arrivant sur un serveur EOLE : `tcpdump -nni $(CreoleGet nom_carte_eth0) port 22`

Des restrictions supplémentaires au niveau des connexions SSH sont disponibles dans l'onglet `Sshd` en mode expert.

Configuration des alias sur l'interface

EOLE supporte les alias sur les cartes réseau. Définir des alias IP consiste à affecter plus d'une adresse IP à une interface.



Pour cela, il faut activer son support (`Ajouter des IP alias sur l'interface à oui`) et configurer l'adresse IP et le masque de sous réseau.

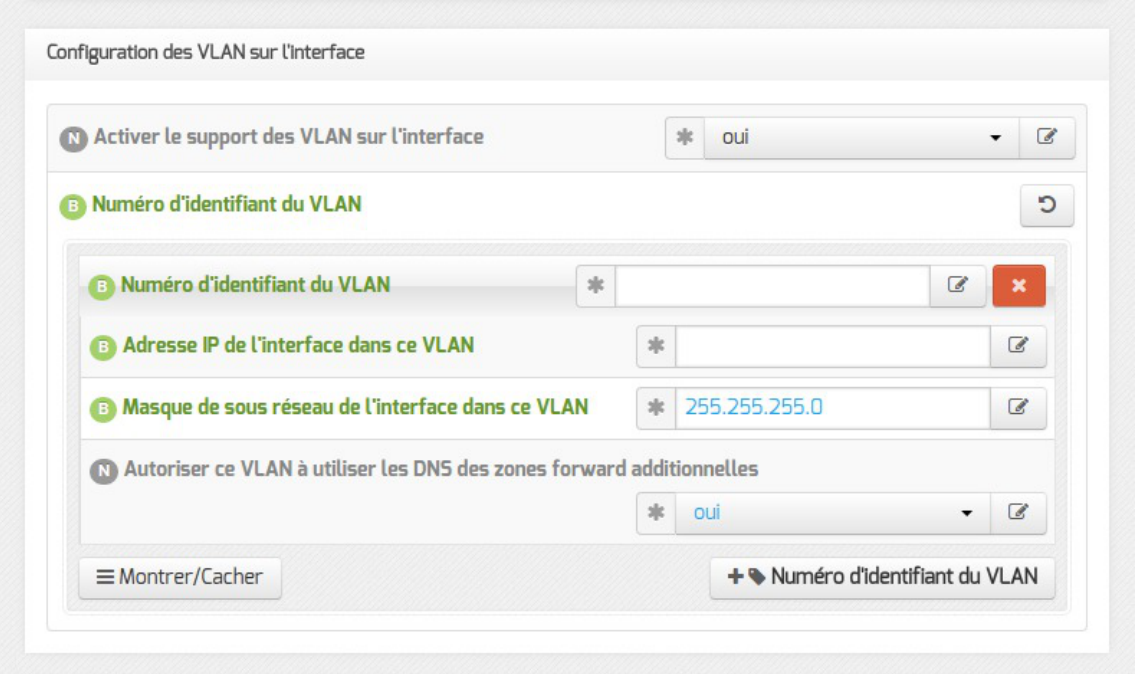
`Autoriser cet alias à utiliser les DNS de zones forward additionnelles` permet d'autoriser le réseau de cet alias à résoudre les noms d'hôte des domaines déclarés dans la section Forward de zone DNS de l'onglet `Zones-dns`.

Si le support du RVP est activé une option supplémentaire est disponible :

- `Autoriser cet alias à utiliser les DNS de Forward RVP/AGRIATES` : Si le service RVP est activé (onglet `Services`) et que le serveur est membre du réseau AGRIATES (onglet `Rvp`) la variable est disponible pour autoriser ou non cet alias à utiliser les DNS noms d'hôte de la zone AGRIATES.

Configuration des VLAN sur l'interface

Il est possible de configurer des VLAN (réseau local virtuel) sur une interface déterminée du module.



Pour cela, il faut activer son support (`Activer le support des VLAN sur l'interface` à `oui` et ajout d'un numéro identifiant du VLAN avec le bouton `+ Numéro d'identifiant du VLAN`) et configurer l'ensemble des paramètres utiles (l'ID, l'adresse IP, ...).

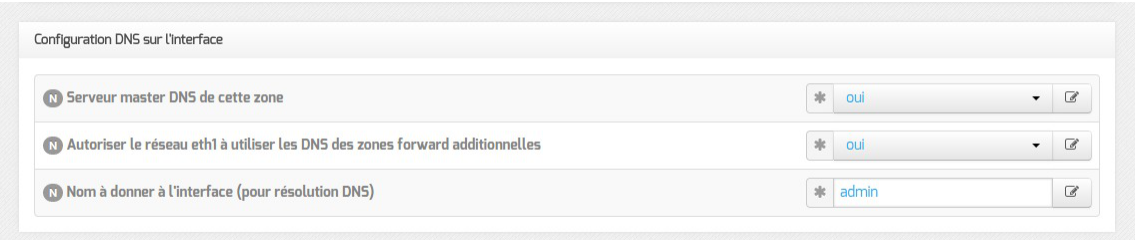
`Autoriser ce VLAN à utiliser les DNS des zones forward additionnelles` permet d'autoriser le réseau de ce VLAN à résoudre les noms d'hôte des domaines déclarés dans la section Forward de zone DNS de l'onglet `Zones-dns`.

Si le support du RVP est activé une option supplémentaire est disponible :

- `Autoriser ce VLAN à utiliser les DNS de Forward RVP/AGRIATES` : Si le service RVP est activé (onglet `Services`) et que le serveur est membre du réseau AGRIATES (onglet `Rvp`) la variable est disponible pour autoriser ou non ce VLAN à utiliser les DNS noms d'hôte de la zone AGRIATES.

Configuration DNS sur l'interface

Il est possible d'ajuster les paramètres du serveur DNS pour chaque interface réseau sauf pour l'interface 0.



- `Serveur master DNS de cette zone` : sert à activer le DNS sur l'interface.
- `Autoriser le réseau ethX à utiliser les DNS des zones forward additionnels` : permet d'autoriser le réseau ethX à résoudre les noms d'hôte des domaines déclarés dans la section `Forward de zone DNS` de l'onglet `Zones-dns`.

- `Nom à donner à l'interface (pour résolution DNS)` : entrée DNS correspondant à l'adresse IP de l'interface ethX. Le nom par défaut (admin pour l'interface eth1) est différent et doit rester pour chaque interface.

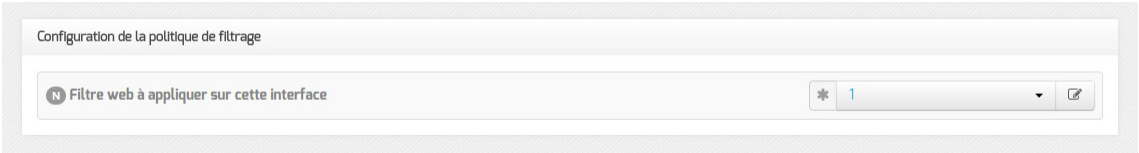
Si le support du RVP est activé une option supplémentaire est disponible :

- `Autoriser le réseau ethX à utiliser les DNS de forward RVP/AGRIATES` : Si le service RVP est activé (onglet `Services`) et que le serveur est membre du réseau AGRIATES (onglet `Rvp`) la variable est disponible pour autoriser ou non le réseau ethX à résoudre les noms d'hôte de la zone AGRIATES.

Configuration de la politique de filtrage

EOLE permet de différencier les zones suivant l'interface (administration ou pédagogie).

La différenciation se fait en modifiant la valeur choisie pour `Filtre Web à appliquer à cette interface` dans la configuration de chaque interface (onglets : `Interface-1`, `Interface-2`, ...).



Les filtres web 1 et 2 correspondent chacun à une instance du logiciel de filtrage. La configuration de chacun des filtres se fait dans l'onglet `Filtrage web`.

Voir aussi...

> Onglet Dansguardian : Configuration du filtrage web

2.7. Onglet Agrégation : Mise en place d'une répartition de charge ou d'une haute disponibilité

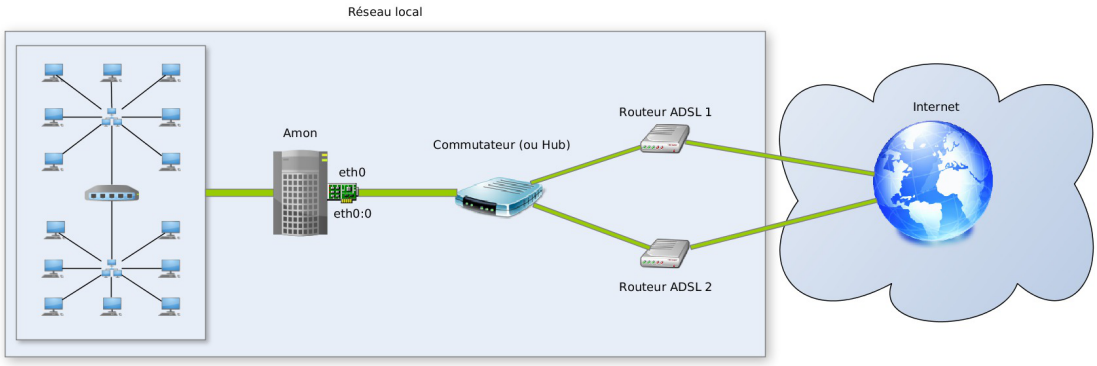
Présentation et mise en place de l'agrégation de liens

L'agrégation de liens permet la mise en place d'une répartition de charge ou d'une haute disponibilité pour les sorties Internet.

Les deux routeurs sont reliés entre eux par un commutateur (ou un Hub) à la carte eth0 du module Amon.

Dans ce cas :

- pas besoin d'utiliser les protocoles d'annonce de routes RIP[p.312] et OSPF[p.310] ;
- il faut un service qui surveille l'état de chacun des liens.



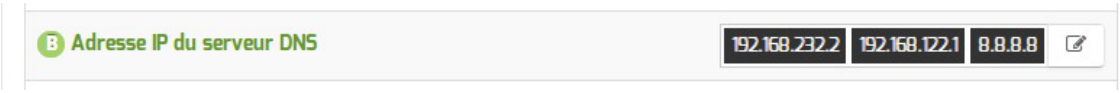
Il est nécessaire d'activer un alias sur l'interface réseau connectée sur l'extérieur pour utiliser ce service.

La configuration de l'agrégation est le résultat de plusieurs contributions de collègues en académie.

La première version a été réalisée par l'académie de Versailles, puis elle a été améliorée successivement par les académies de Nantes et de Lyon.

Onglet Général

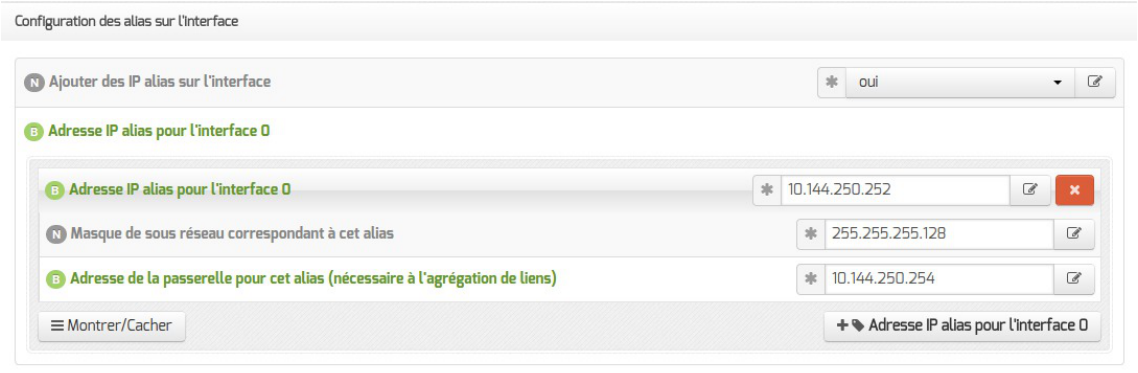
Dans la section `Adresse IP du serveur DNS` de l'onglet Général, ajouter les adresses des serveurs DNS de chacun des fournisseurs, en plaçant, de préférence, le DNS du premier lien en première position.



Onglet Interface-0

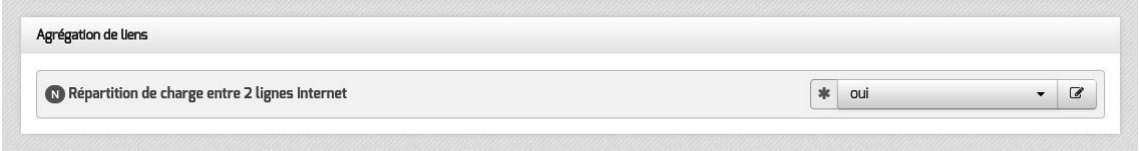
Il faut, en premier lieu, déclarer un alias sur l'interface eth0 dans la section `Configuration des alias sur l'interface`.

Les paramètres réseaux (IP, masque et passerelle) doivent être ceux attribués par le fournisseur d'accès du second lien.



Création d'un alias sur eth0 pour l'agrégation de liens

L'activation d'un alias IP, fait apparaître un nouveau paramètre, `Répartition de charge entre 2 lignes Internet`, qu'il faut passer à `oui`.

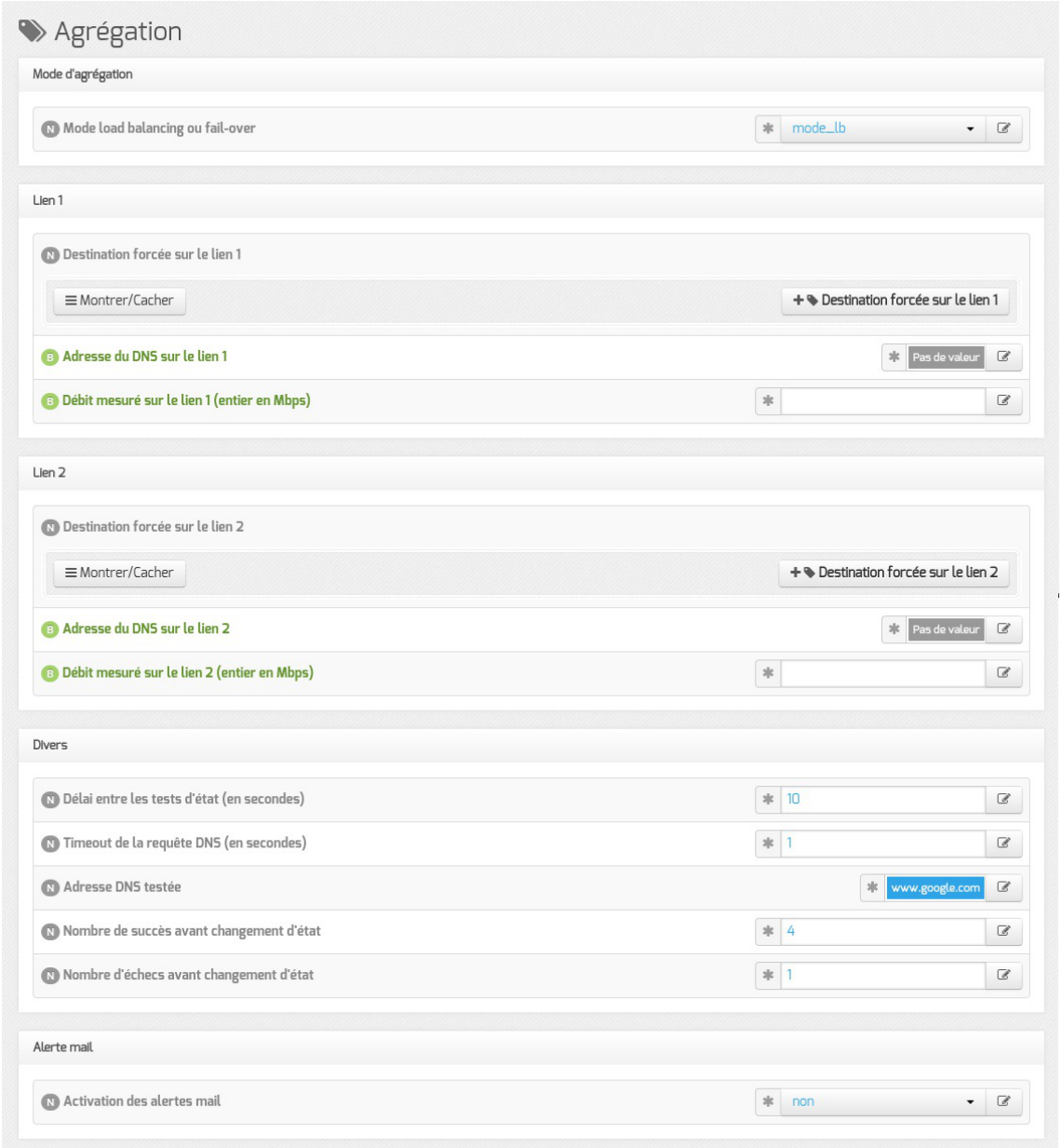


Activation de l'agrégation de lien

Un nouvel onglet, `Agrégation`, est disponible.

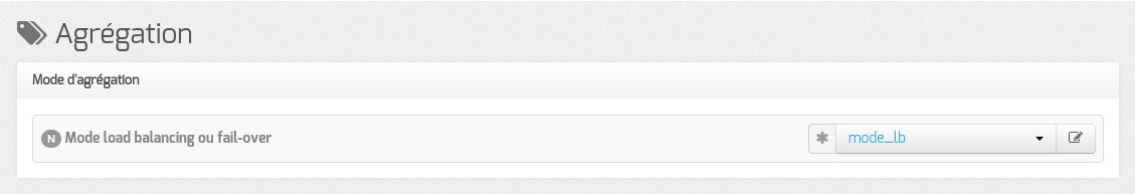
Onglet Agrégation : Configuration de l'agrégation de liens

Pour avoir accès à l'onglet concernant l'agrégation, il faut avoir activé la `Répartition de charge entre 2 lignes Internet` dans l'onglet `Interface-0` comme expliqué précédemment.



Paramétrage de l'agrégation de liens

Modes d'agrégation



Il existe deux modes d'agrégation :

- le mode `mode-lb` (pour load balancing) correspond à la répartition de charge et fonctionne avec la notion de poids à utiliser sur les différentes passerelles ;
- le mode `mode-fo`, (pour fail-over) un seul lien est utilisé à la fois, il n'y a plus de notion de poids et il n'y a plus qu'une seule route par défaut.

Dans les deux modes il est possible de forcer des destinations IP ou réseau, et dans les deux cas si un lien tombe tous les flux (et également les destinations forcées) sont redirigés vers le second lien.

Quand les deux liens sont fonctionnels, on se retrouve dans la configuration de départ.

Le VPN, de par son mode de fonctionnement, ne peut pas être réparti entre plusieurs abonnements.

Tout le trafic devant passer par un seul lien, il est nécessaire d'utiliser le mécanisme de destination forcée.

Que le `Lien 1` ou le `Lien 2` soit choisi pour faire transiter le VPN, s'il devient indisponible, le VPN ne fonctionnera plus.

Adresse des DNS

Les champs `Adresse du DNS sur le lien 1` et `Adresse du DNS sur le lien 2` sont des champs obligatoires pour le bon fonctionnement de l'agrégation.

Les adresses DOIVENT être différentes sur chaque lien car c'est avec ces DNS que se font les tests d'état des liens.

Adresse DNS testée

Il est possible de spécifier plusieurs mires de tests qui seront testées afin de déterminer l'état des liens (résolution DNS avec le serveur DNS de chacun des liens).

L'ensemble des DNS doit être déclaré dans l'onglet `Général`.

Alerte mail

Lorsque l'un des liens est coupé, le message suivant est envoyé : `Seul le lien 2 est actif, redirection des flux sur ce lien`.

Quand les deux liens sont de nouveaux fonctionnels, le message suivant est envoyé : `Rechargement de la répartition sur les 2 liens`.

2.8. Onglet Clamav : Configuration de l'anti-virus

EOLE propose un service anti-virus réalisé à partir du logiciel libre Clamav.

http://www.clamav.net

Activation de l'anti-virus

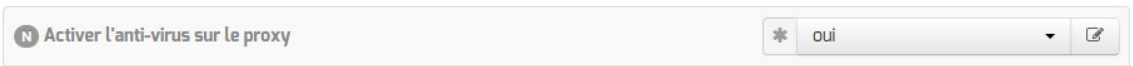
L'onglet `Clamav` n'est accessible que si le service est activé dans l'onglet `Services`. Pour ce faire, passer la variable `Activer l'anti-virus ClamAV` à `oui`.

Sur le module Amon, il n'est possible d'activer l'anti-virus que sur le proxy et sur la messagerie.

Si aucun service n'utilise l'anti-virus, il est utile de le désactiver dans l'onglet `Services`. Il faut passer la variable `Activer l'anti-virus ClamAV` à `non`. L'onglet `Clamav` n'est alors plus visible.

Activation de l'anti-virus sur le proxy

Pour activer l'anti-virus en temps réel sur les fichiers filtrés par le proxy Internet, il faut passer la variable `Activer l'anti-virus sur le proxy` à `oui` dans l'onglet `Clamav`.

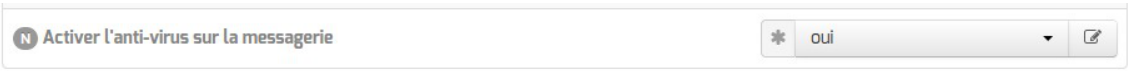


L'anti-virus sur le proxy permet d'analyser le trafic HTTP mais ne saurait en aucun cas remplacer la présence d'un anti-virus sur les postes clients.

L'anti-virus activé sur le proxy utilise beaucoup de ressources CPU[p.303]. Il peut donc affecter les performances du pare-feu et considérablement ralentir la navigation.

Activation de l'anti-virus sur la messagerie

Pour activer l'anti-virus sur la messagerie il faut passer la variable `Activer l'antivirus sur la messagerie` à `oui` dans l'onglet `Clamav`.



Contribuer

La base de données de virus est mise à jour avec l'aide de la communauté.

Il est possible de faire des signalements :

- signaler de nouveaux virus qui ne sont pas détectés par ClamAV ;
- signaler des fichiers propres qui ne sont pas correctement détectés par ClamAV (faux-positif).

Pour cela il faut utiliser le formulaire suivant (en) : http://cgi.clamav.net/sendvirus.cgi

L'équipe de ClamAV examinera votre demande et mettra éventuellement à jour la base de données.

En raison d'un nombre élevé de déposants, il ne faut pas soumettre plus de deux fichiers par jour.

Il ne faut pas signaler des PUA[p.312] comme étant des faux positifs.

2.9. Onglet Relai DHCP

Pour des raisons de sécurité, le service DHCP[p.303] n'a pas, à priori, à être installé sur le module Amon.

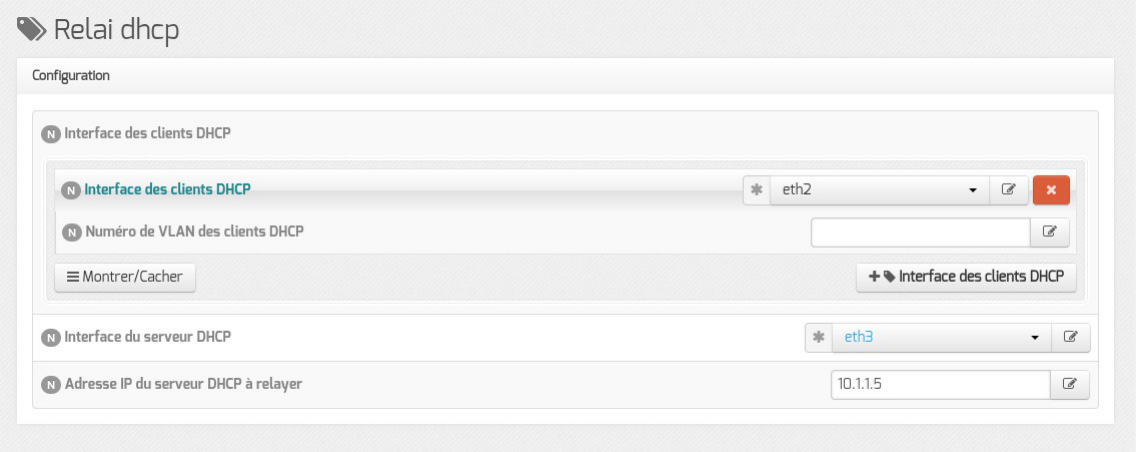
Il vaut mieux utiliser un autre module (module Scribe ou module Horus par exemple) pour fournir ce service.

Le protocole DHCP fonctionne en utilisant un mécanisme de broadcast[p.302].

De ce fait, les trames ne sont, par défaut, pas routables d'un réseau vers un autre.

Si le serveur DHCP ne se situe pas sur la même zone que les stations, il faut mettre en place un relai DHCP.

L'onglet `Relai dhcp` n'est accessible que si le service est activé dans l'onglet `Services`. Pour ce faire, passer la variable `Activer le relai DHCP` à `oui`.



Vue de l'onglet Relai dhcp de l'interface de configuration du module

Dans la configuration ci-dessus (4zones), on déclare que l'on veut relayer le DHCP du module Scribe (adresse IP : 10.1.1.5) qui se trouve dans la DMZ (eth3 est la 4ème interface) vers le réseau pédagogique (eth2 est la 3ème interface).

Il est possible de restreindre le relayage sur un VLAN[p.314] particulier en renseignant son numéro dans la variable `Numéro de VLAN des clients DHCP`.

Grâce au découpage des paquets par services, la mise en œuvre d'un DHCP sur le module Amon, bien que déconseillée, est facilitée par le paquet `eole-dhcp`.

Voir aussi...

- eole-dhcp
- Configuration du module Amon avec le module Scribe en DMZ [p.187]

2.10. Onglet Onduleur

Sur chaque module EOLE, il est possible de configurer votre onduleur.

Le logiciel utilisé pour la gestion des onduleurs est NUT[p.309]. Il permet d'installer plusieurs clients sur le même onduleur. Dans ce cas, une machine aura le contrôle de l'onduleur (le maître/master) et en cas de coupure, lorsque la charge de la batterie devient critique, le maître indiquera aux autres machines (les esclaves) de s'éteindre avant de s'éteindre lui-même.

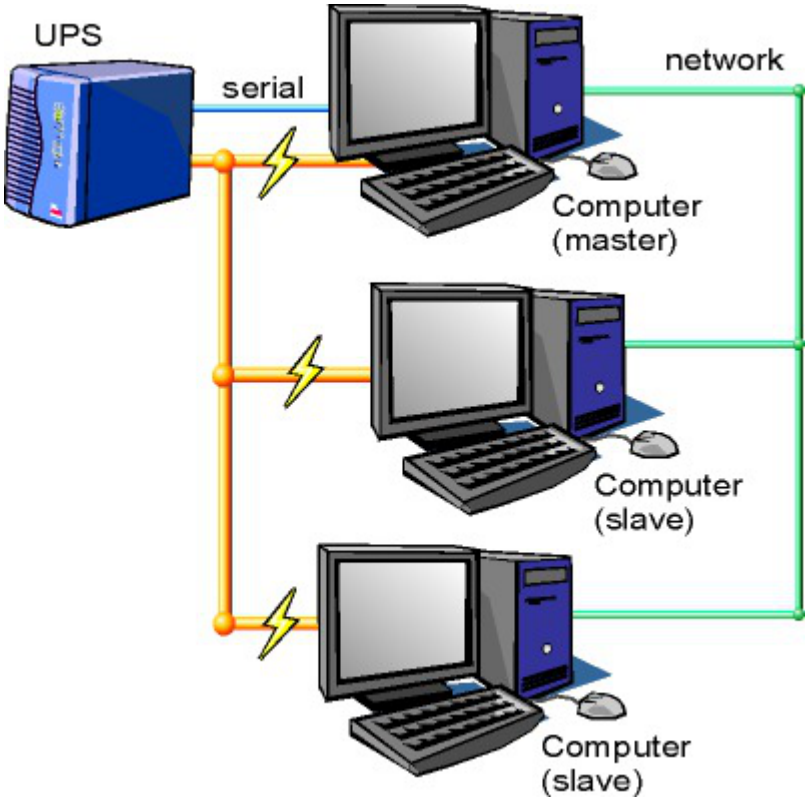


Schéma d'Olivier Van Hoof sous licence GNU FDL Version 1.2 - http://ovanhoof.developpez.com/upsusb/

Certains onduleurs sont assez puissants pour alimenter plusieurs machines.

http://www.networkupstools.org/

Le projet offre une liste de matériel compatible avec le produit mais cette liste est donnée pour la dernière version du produit :

http://www.networkupstools.org/stable-hcl.html

Pour connaître la version de NUT qui est installée sur le module :

```
# apt-cache policy nut
```

ou encore :

```
# apt-show-versions nut
```

Si la version retournée est 2.7.1 on peut trouver des informations sur la prise en charge du matériel dans les notes de version à l'adresse suivante :

http://www.networkupstools.org/source/2.7/new-2.7.1.txt

Si le matériel n'est pas dans la liste, on peut vérifier que sa prise en charge soit faite par une version plus récente et donc non pris en charge par la version actuelle :

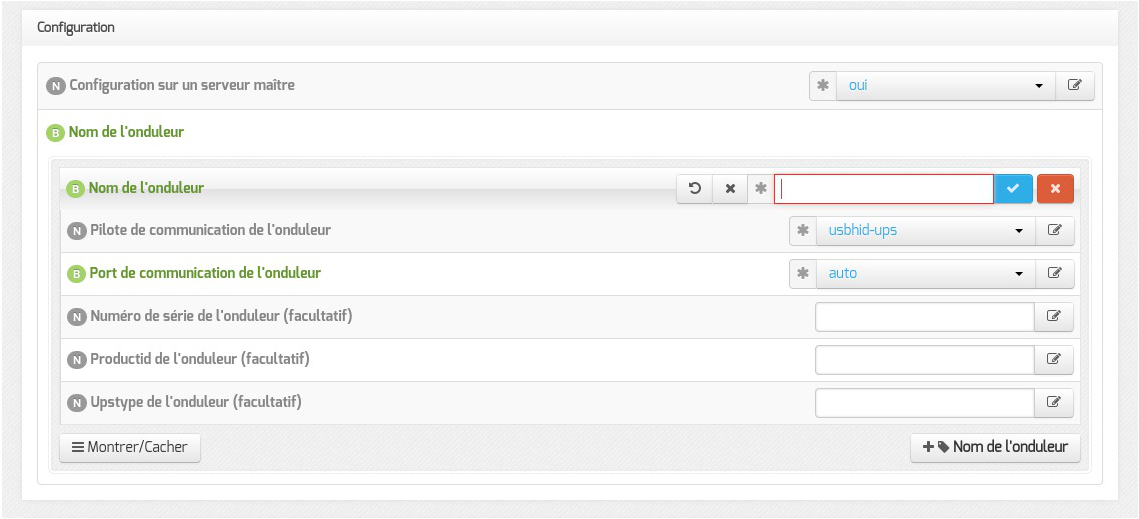
http://www.networkupstools.org/source/2.7/new-2.7.3.txt

L'onglet `Onduleur` n'est accessible que si le service est activé dans l'onglet `Services`.

Vue de l'onglet Onduleur

Si l'onduleur est branché directement sur le module il faut laisser la variable `Configuration sur un serveur maître` à `oui`, cliquer sur le bouton `+ Nom de l'onduleur` et effectuer la configuration liée au serveur maître.

La configuration sur un serveur maître



Même si le nom de l'onduleur n'a aucune conséquence, il est obligatoire de remplir cette valeur dans le champ `Nom pour l'onduleur`.

Il faut également choisir le nom du pilote de l'onduleur dans la liste déroulante `Pilote de communication de l'onduleur` et éventuellement préciser le `Port de communication` si l'onduleur n'est pas USB.

Les champs `Numéro de série de l'onduleur`, `Productid de l'onduleur` et `Upstype de l'onduleur` sont facultatifs si il n'y a pas de serveur esclave. Il n'est nécessaire d'indiquer ce numéro de série que dans le cas où le serveur dispose de plusieurs onduleurs et de serveurs esclaves.

Le nom de l'onduleur ne doit contenir que des chiffres ou des lettres en minuscules : *[a-z][0-9]* sans espaces, ni caractères spéciaux.

Configuration d'un second onduleur sur un serveur maître

Si le serveur dispose de plusieurs alimentations, il est possible de les connecter chacune d'elle à un onduleur différent.

Il faut cliquer sur le bouton `+ Nom de l'onduleur` pour ajouter la prise en charge d'un onduleur supplémentaire dans l'onglet `Onduleur` de l'interface de configuration du module.

Si les onduleurs sont du même modèle et de la même marque, il faut ajouter de quoi permettre au pilote NUT de les différencier.

Cette différenciation se fait par l'ajout d'une caractéristique unique propre à l'onduleur. Ces caractéristiques dépendent du pilote utilisé, la page de `man` du pilote vous indiquera lesquelles sont disponibles.

Exemple pour le pilote Solis :

```
# man solis
```

Afin de récupérer la valeur il faut :

- ne connecter qu'un seul des onduleurs ;
- le paramétrer comme indiqué dans la section précédente ;
- exécuter la commande : `upsc <nomOnduleurDansGenConfig>@localhost|grep <nom_variable>` ;
- débrancher l'onduleur ;
- brancher l'onduleur suivant ;
- redémarrer `nut` avec la commande : `# service nut restart` ;
- exécuter à nouveau la commande pour récupérer la valeur de la variable.

Une fois les numéros de série connus, il faut les spécifier dans les champ `Numéro de série de l'onduleur` de chaque onduleur.

Deux onduleurs de même marque

Pour deux onduleurs de marque MGE, reliés à un module Scribe par câble USB, il est possible d'utiliser la valeur "serial", voici comment la récupérer :

```
# upsc <nomOnduleurDansGenConfig>@localhost | grep serial
driver.parameter.serial: AV4H4601W
ups.serial: AV4H4601W
```

Deux onduleurs différents

Un onduleur sur port série :

- Nom de l'onduleur : `eoleups` ;
- Pilote de communication de l'onduleur : `apcsmart` ;
- Port de communication de l'onduleur : `/dev/ttyS0`.

Si l'onduleur est branché sur le port série (en général : `/dev/ttyS0`), les droits doivent être adaptés.

Cette adaptation est effectuée automatiquement lors de l'application de la configuration.

Onduleur sur port USB :

- Nom de l'onduleur : `eoleups` ;

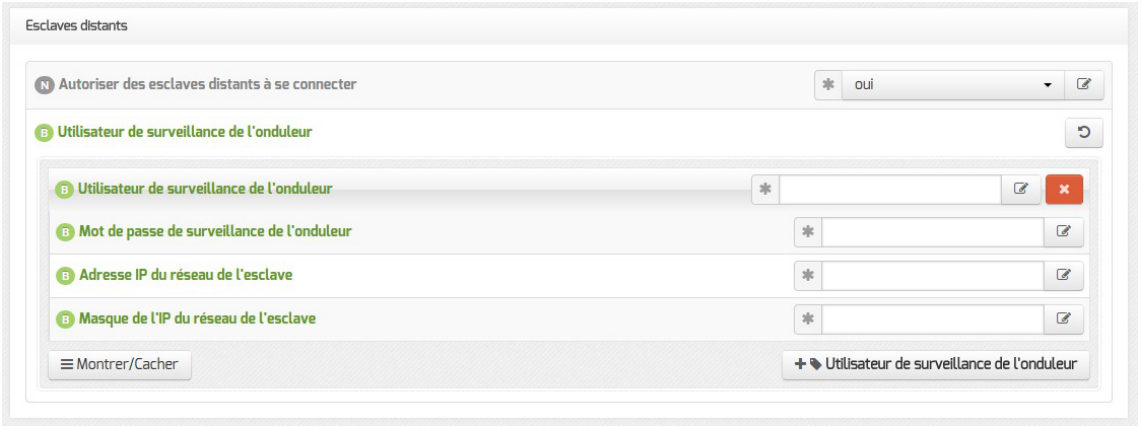
- Pilote de communication de l 'onduleur : `usbhid-ups` ;
- Port de communication de l'onduleur : `auto`.

La majorité des onduleurs USB sont détectés automatiquement.

Attention, seul le premier onduleur sera surveillé.

Autoriser des esclaves distants à se connecter

Pour déclarer un serveur esclave, il faut passer la variable `Autoriser des esclaves distants à se connecter` à `oui` puis ajouter un utilisateur sur le serveur maître afin d'autoriser l'esclave a se connecter avec cet utilisateur.



Idéalement, il est préférable de créer un utilisateur différent par serveur même s'il est possible d'utiliser un unique utilisateur pour plusieurs esclaves. Pour configurer plusieurs utilisateurs il faut cliquer sur le bouton `+ Utilisateur de surveillance de l'onduleur`.

Pour chaque utilisateur, il faut saisir :

- un `Utilisateur de surveillance de l'onduleur` ;
- un `Mot de passe de surveillance de l'onduleur` associé à l'utilisateur précédemment créé ;
- l'`Adresse IP du réseau de l'esclave` (cette valeur peut être une adresse réseau plutôt qu'une adresse IP) ;
- le `Masque de l'IP du réseau de l'esclave` (comprendre le masque du sous réseau de l'adresse IP de l'esclave)

Le nom de l'onduleur ne doit contenir que des chiffres ou des lettres en minuscules : *[a-z][0-9]* sans espaces, ni caractères spéciaux.

Chaque utilisateur doit avoir un nom différent.

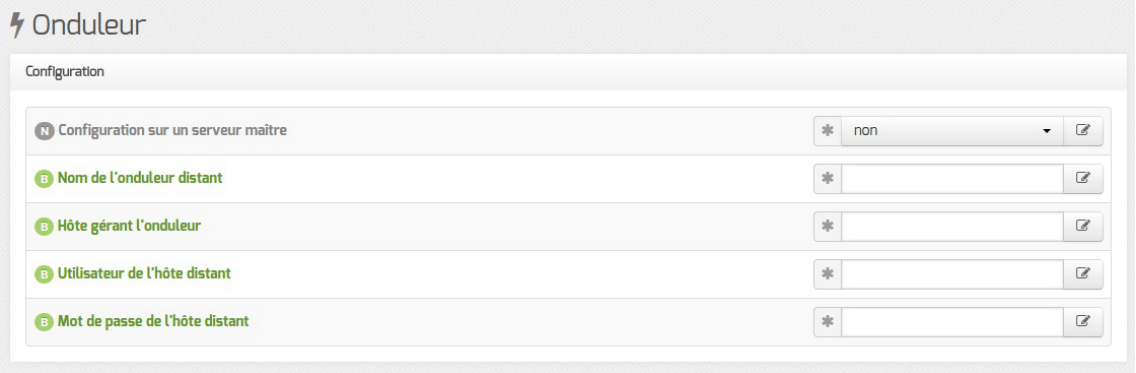
Les noms `root` et `localmonitor` sont réservés.

Pour plus d'informations, vous pouvez consulter la page de manuel : `man ups.conf` ou consulter la page web suivante : http://manpages.ubuntu.com/manpages/trusty/en/man5/ups.conf.5.html

Configurer un serveur esclave

Une fois qu'un serveur maître est configuré et fonctionnel, il est possible de configurer le ou les serveurs esclaves.

Pour configurer le module en tant qu'esclave, il faut activer le service dans l'onglet `Services` puis, dans l'onglet `Onduleur`, passer la variable `Configuration sur un serveur maître` à `non`.



Il faut ensuite saisir les paramètres de connexion à l'hôte distant :

- le `Nom de l'onduleur distant` (valeur renseignée sur le serveur maître) ;
- l'`Hôte gérant l'onduleur` (adresse IP ou nom d'hôte du serveur maître) ;
- l'`Utilisateur de l'hôte distant` (nom d'utilisateur de surveillance créé sur le serveur maître) ;
- le `Mot de passe de l'hôte distant` (mot de passe de l'utilisateur de surveillance créé sur le serveur maître).

Exemple de configuration

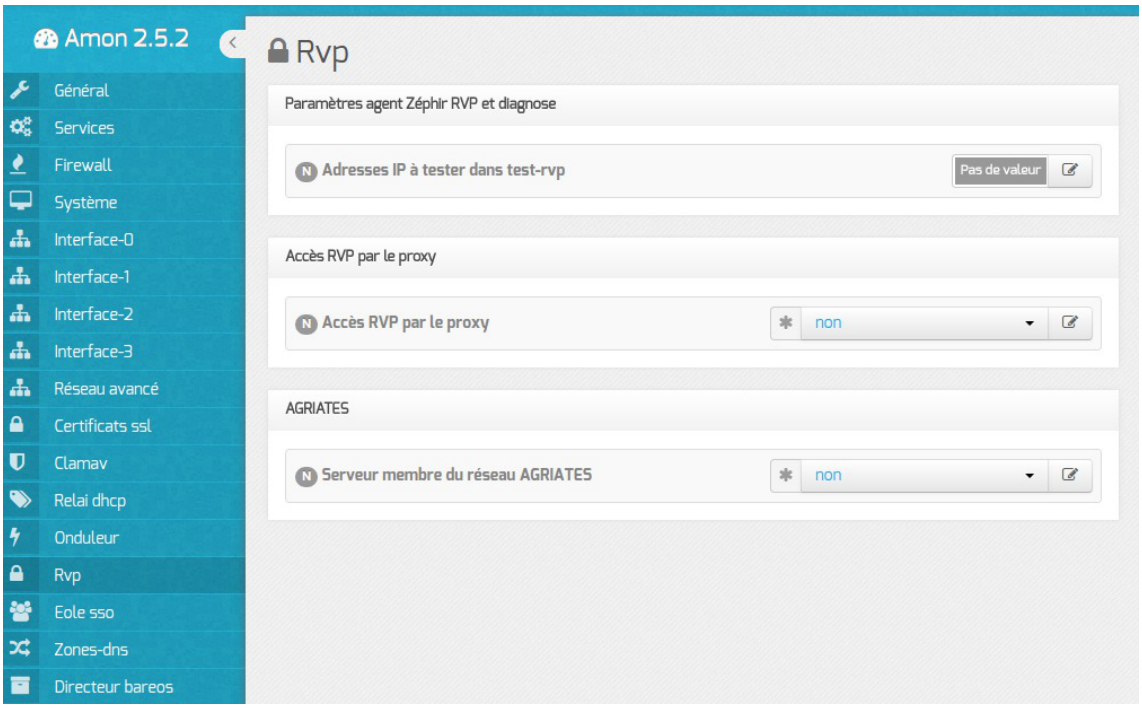
Sur le serveur maître :

- Nom de l'onduleur : `eoleups` ;
- Pilote de communication de l'onduleur : `usbhid-ups` ;
- Port de communication de l'onduleur : `auto` ;
- Utilisateur de surveillance de l'onduleur : `scribe` ;
- Mot de passe de surveillance de l'onduleur : `99JJUE2EZOAI2IZI10IIZ93I187UZ8` ;
- Adresse IP du réseau de l'esclave : `192.168.30.20` ;
- Masque de l'IP du réseau de l'esclave : `255.255.255.255`.

Sur le serveur esclave :

- Nom de l'onduleur distant : `eoleups` ;
- Hôte gérant l'onduleur : `192.168.30.10` ;
- Utilisateur de l'hôte distant : `scribe` ;
- Mot de passe de l'hôte distant : `99JJUE2EZOAI2IZI10IIZ93I187UZ8`.

2.11. Onglet Rvp : Mettre en place le réseau virtuel privé

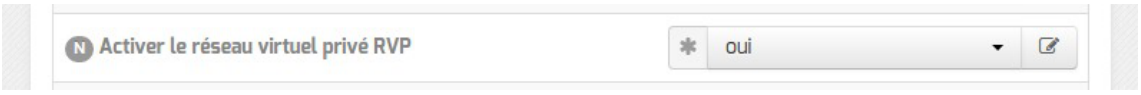


Onglet Rvp mode Normal

Le réseau virtuel privé[p.312] (RVP) peut être activé au moment de la configuration et de l'instanciation d'un module Amon ou sur des modules Amon déjà en exploitation.

Mise en place du RVP

L'onglet `Rvp` apparaît après activation du service dans l'onglet `Services`.



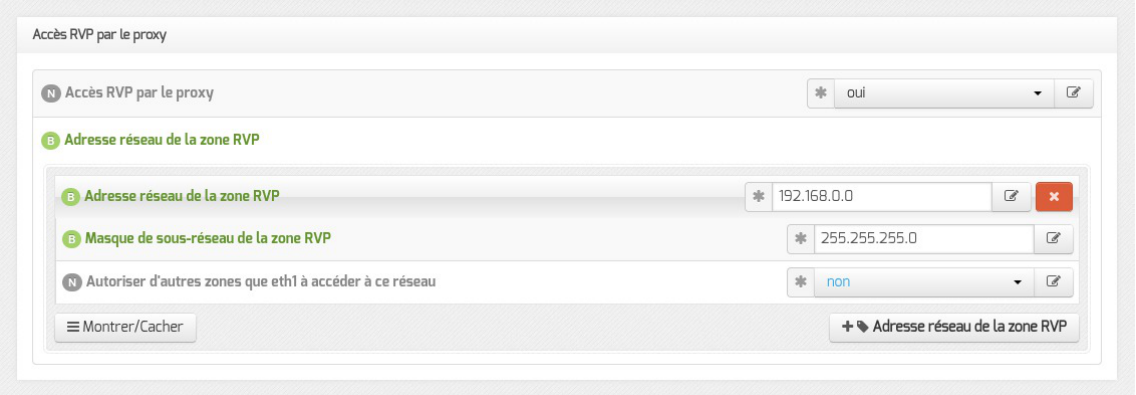
Configuration des tunnels

Le mode VPN database n'est plus supporté et n'est plus disponible à partir de la version 2.5.1 du module Amon. La configuration des tunnels s'effectue d'office en mode fichier plat.

À l'occasion de la mise en place d'un nouveau tunnel avec un serveur Sphynx inférieur à la version EOLE 2.5, il faudra impérativement configurer ce serveur Sphynx en mode database à non.

Accès RVP par le proxy

Pour paramétrer l'accès RVP par le proxy, il faut passer la variable `Accès RVP par le proxy` à `oui`.

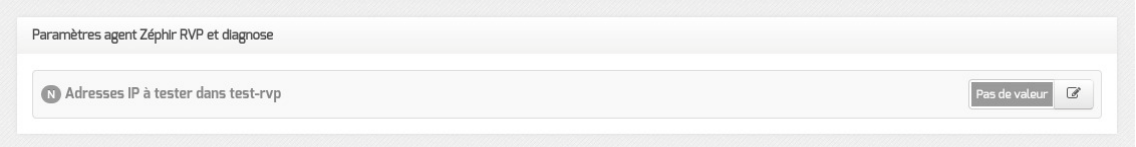


L'adresse réseau de la zone RVP permet la configuration du proxy Squid pour autoriser ou non, aux postes autres que sur l'interface eth1, l'accès via le VPN à un sous réseau.

Pour ajouter d'autres adresses réseau il faut cliquer sur le bouton `+Adresse réseau de la zone RVP`.

Paramètres agent Zéphir RVP et diagnose

Le champ `Adresses IP à tester dans test-rvp` permet de saisir une ou plusieurs adresses IP qui seront utilisées par le diagnose et par l'agent Zéphir pour tester des adresses IP à l'autre extrémité des tunnels.



AGRIATES

Si le serveur est membre d'AGRIATES il faut passer la variable `Serveur membre du réseau AGRIATES` à `oui`.

- `Adresse du DNS permettant de résoudre les in.ac-acad.fr` permet de spécifier l'adresse IP du serveur DNS permettant de résoudre les noms de zone AGRIATES (in.ac-académie.fr) ;
- `Nom DNS de la zone résolue par le DNS AGRIATES` : permet de spécifier d'autres noms de zones résolues par le DNS AGRIATES.

Application de la configuration et gestion du RVP

Activation du RVP au moment de l'instanciation du serveur Amon

Au lancement de l'instanciation, la question suivante vous est posée :

`Voulez-vous configurer le Réseau Virtuel Privé maintenant ? [oui/non] [non] :`

Vous devez répondre `oui` à cette question.

Deux choix sont alors proposés :

`1.Manuel` permet de prendre en compte la configuration RVP présente sur une clé USB ;

`2.Zéphir` active la configuration RVP présente sur le serveur Zéphir. Cela suppose que le serveur est déjà enregistré sur Zéphir. Il sera demandé un compte Zéphir et son code secret ainsi que l'identifiant Zéphir du serveur Sphynx auquel associer le module Amon.

Dans les deux cas, le code secret de la clé privée est demandée. Si le code secret est correct le RVP est configuré pour cette machine et l'instanciation peut se poursuivre...

Activation du RVP sur des modules Amon déjà en exploitation

Pour activer un RVP sur un module Amon déjà instancié, il faut lancer en tant qu'utilisateur `root` la commande `active_rvp init`.

Suppression du RVP

Pour supprimer un RVP, il faut lancer en tant qu'utilisateur `root` la commande `active_rvp delete`.

2.12. Onglet Eole sso : Configuration du service SSO pour l'authentification unique

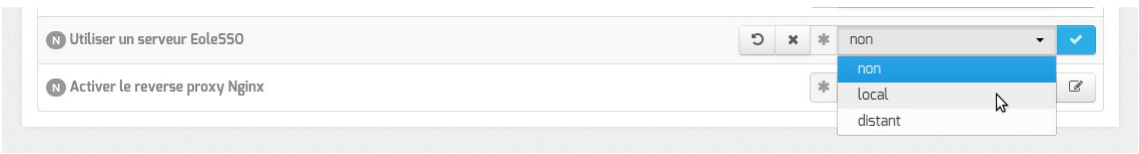
Le serveur EoleSSO est prévu pour être déployé sur un module EOLE.

Il est cependant possible de l'utiliser dans un autre environnement en modifiant manuellement le fichier de configuration `/usr/share/sso/config.py`.

Cette section décrit la configuration du serveur depuis l'interface de configuration du module disponible sur tous les modules EOLE. Les valeurs définies par défaut simplifient la configuration dans le cadre d'une utilisation prévue sur les modules EOLE.

Serveur local ou distant

L'activation du serveur EoleSSO s'effectue dans l'onglet `Services`.



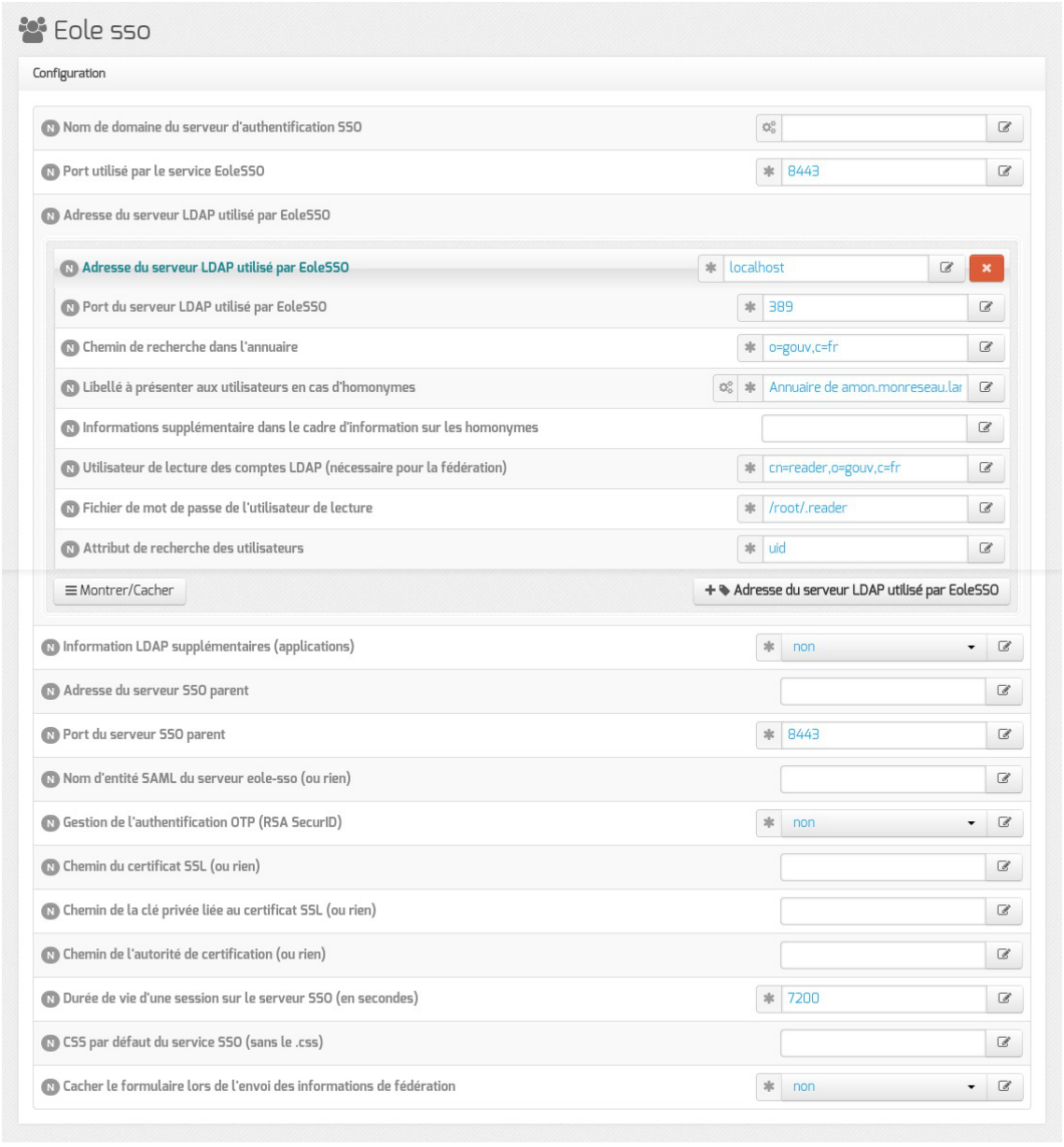
Activation du serveur SSO dans l'interface de configuration du module

La variable `Utiliser un serveur EoleSSO` permet :

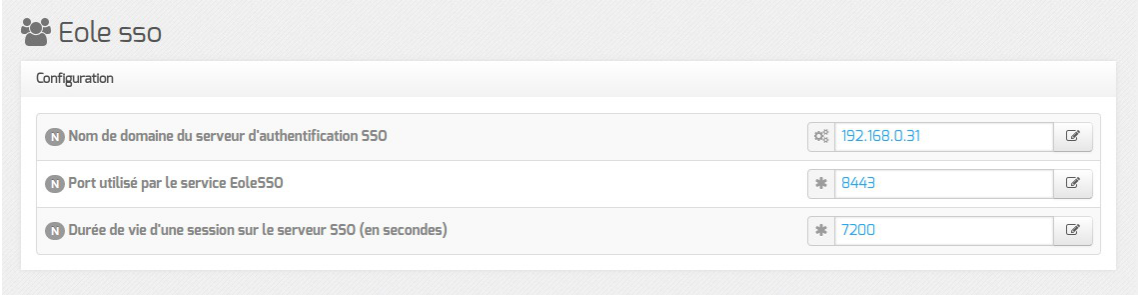
- `non` : de ne pas utiliser de SSO sur le serveur ;
- `local` : d'utiliser et de configurer le serveur EoleSSO local ;
- `distant` : d'utiliser un serveur EoleSSO distant (configuration cliente).

Adresse et port d'écoute

L'onglet supplémentaire `Eole-sso` apparaît si l'on a choisi d'utiliser un serveur EoleSSO local ou distant.



Dans le cas de l'utilisation d'un serveur EoleSSO distant, seuls les paramètres `Nom de domaine du serveur d'authentification SSO` et `Port utilisé par le service EoleSSO` sont requis et les autres options ne sont pas disponibles car elles concernent le paramétrage du serveur local.



Dans le cas de l'utilisation du serveur EoleSSO local, `Nom de domaine du serveur d'authentification SSO` doit être renseigné avec le nom DNS du serveur.

Par défaut le serveur communique sur le port `8443`. Il est conseillé de laisser cette valeur par défaut en cas d'utilisation avec d'autres modules EOLE.

Si vous décidez de changer ce port, pensez à le changer également dans la configuration des autres machines l'utilisant.

Configuration LDAP

Le serveur EoleSSO se base sur des serveurs LDAP pour authentifier les utilisateurs et récupérer leurs attributs.

Il est possible ici de modifier les paramètres d'accès à ceux-ci :

- l'adresse et le port d'écoute du serveur LDAP ;
- le chemin de recherche correspond à l'arborescence de base dans laquelle rechercher les utilisateurs ;
- un libellé à afficher dans le cas où un utilisateur aurait à choisir entre plusieurs annuaires/établissements pour s'authentifier (voir le chapitre `Gestion des sources d'authentifications multiples`) ;
- un fichier d'informations à afficher dans le cadre qui est présenté en cas d'homonymes. Ces informations apparaîtront si l'utilisateur existe dans l'annuaire correspondant. Les fichiers doivent être placés dans le répertoire `/usr/share/sso/interface/info_homonymes` ;
- DN et mot de passe d'un utilisateur en lecture pour cet annuaire ;
- attribut de recherche des utilisateurs : indique l'attribut à utiliser pour rechercher l'entrée de l'utilisateur dans l'annuaire (par défaut, uid)
- choix de la disponibilité ou non de l'authentification par clé OTP[p.310] si disponible *(voir plus loin)*.

Dans le cas où vous désirez fédérer EoleSSO avec d'autres fournisseurs de service ou d'identité (ou 2 serveurs EoleSSO entre eux), il est nécessaire de configurer un utilisateur ayant accès en lecture au serveur LDAP configuré.

Il sera utilisé pour récupérer les attributs des utilisateurs suite à réception d'une assertion d'un fournisseur d'identité (ou dans le cas d'une authentification par OTP).

Cet utilisateur est pré-configuré pour permettre un accès à l'annuaire local sur les serveurs EOLE.

Sur les modules EOLE, la configuration recommandée est la suivante :

- utilisateur : `cn=reader,o=gouv,c=fr`
- fichier de mot de passe : /root/.reader

Si vous connectez EoleSSO à un annuaire externe, vous devez définir vous même cet utilisateur :

- `Utilisateur de lecture des comptes ldap` : renseignez son *dn* complet dans l'annuaire
- `fichier de mot de passe de l'utilisateur de lecture` : entrez le chemin d'un fichier ou vous stockerez son mot de passe (modifiez les droits de ce fichier pour qu'il soit seulement accessible par l'utilisateur `root`)

Serveur SSO parent

Un autre serveur EoleSSO peut être déclaré comme serveur parent dans la configuration (adresse et port). Se reporter au chapitre traitant de la fédération pour plus de détails sur cette notion.

Si un utilisateur n'est pas connu dans le référentiel du serveur EoleSSO, le serveur essayera de l'authentifier auprès de son serveur parent (dans ce cas, la liaison entre les 2 serveurs se fait par l'intermédiaire d'appels XML-RPC[p.315] en HTTPS, sur le port défini pour le serveur EoleSSO).

Si le serveur parent authentifie l'utilisateur, il va créer un cookie de session local et rediriger le navigateur client sur le serveur parent pour qu'une session y soit également créée (le cookie de session est accessible seulement par le serveur l'ayant créé).

Ce mode de fonctionnement n'est plus recommandé aujourd'hui. Il faut préférer à cette solution la mise en place d'une fédération par le protocole SAML.

Prise en compte de l'authentification OTP

Il est possible de configurer EoleSSO pour gérer l'authentification par clé OTP à travers le protocole securID[p.312] de la société EMC (précédemment RSA).

Pour cela il faut :

- installer et configurer le client PAM/Linux proposé par EMC (voir annexes)
- Répondre `oui` à la question `Gestion de l'authentification OTP (RSA SecurID)`

Des champs supplémentaires apparaissent :

- Pour chaque annuaire configuré, un champ permet de choisir la manière dont les identifiants à destination du serveur OTP sont gérés. '`inactifs`' (par défaut) indique que l'authentification OTP n'est pas proposée à l'utilisateur. Avec `'identiques'`, le login local (LDAP) de l'utilisateur sera également utilisé comme login OTP. La dernière option est '`configurables`', et indique que les utilisateurs doivent renseigner eux même leur login OTP. Dans ce dernier cas, l'identifiant est conservé sur le serveur EoleSSO pour que l'utilisateur n'ait pas à le renseigner à chaque fois (fichier /usr/share/sso/securid_users/securid_users.ini).
- Le formulaire d'authentification détecte automatiquement si le mot de passe entré est un mot de passe OTP. Il est possible de modifier la reconnaissance si elle ne convient pas en réglant les tailles

minimum et maximum du mot de passe et en donnant une expression régulière qui sera vérifiée si la taille correspond. Les options par défaut correspondent à un mot de passe de 10 à 12 caractères uniquement numériques.

Certificats

Les communications de et vers le serveur EoleSSO sont chiffrées.

Sur les modules EOLE, des certificats auto-signés sont générés à l'instanciation[p.306] du serveur et sont utilisés par défaut.

Il est possible de renseigner un chemin vers une autorité de certification et un certificat serveur dans le cas de l'utilisation d'autres certificats (par exemple, des certificat signés par une entité reconnue).

Les certificats doivent être au format PEM.

Fédération d'identité

Le serveur EoleSSO permet de réaliser une fédération vers un autre serveur EoleSSO ou vers d'autre types de serveurs compatibles avec le protocole SAML[p.312] (version 2).

`Nom d'entité SAML du serveur eole-sso (ou rien)` : nom d'entité du serveur EoleSSO local à indiquer dans les messages SAML. Si le champ est laissé à vide, une valeur est calculée à partir du nom de l'académie et du nom de la machine.

`Cacher le formulaire lors de l'envoi des informations de fédération` : permet de ne pas afficher le formulaire de validation lors de l'envoi des informations de fédération à un autre système. Ce formulaire est affiché par défaut et indique la liste des attributs envoyés dans l'assertion SAML permettant la fédération.

Autres options

`Durée de vie d'une session (en secondes)` : indique la durée de validité d'une session SSO sur le serveur. Cela n'influence pas la durée de la session sur les applications authentifiées, seulement la durée de la validité du cookie utilisé par le serveur SSO. Au delà de cette durée, l'utilisateur devra obligatoirement se ré-authentifier pour être reconnu par le serveur SSO. Par défaut, la durée de la session est de 3 heures (7200 secondes).

`CSS par défaut du service SSO (sans le .css)` : permet de spécifier une CSS différente pour le formulaire d'authentification affiché par le serveur EoleSSO. Le fichier CSS doit se trouver dans le répertoire `/usr/share/sso/interface/theme/style/<nom_fichier>.css`. *Se reporter au chapitre personnalisation pour plus de possibilités à ce sujet*.

Voir aussi...

> Gestion des sources d'authentification multiples

2.13. Onglet Messagerie

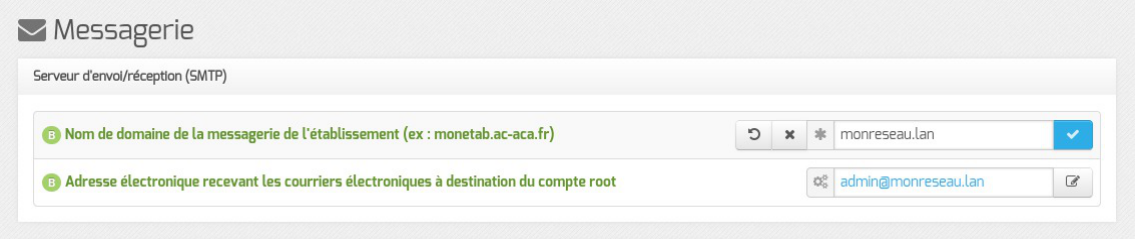
Même sur les modules ne fournissant aucun service directement lié à la messagerie, il est nécessaire de configurer une passerelle SMTP valide car de nombreux outils sont susceptibles de nécessiter l'envoi de

mails.

La plupart des besoins concernent l'envoi d'alertes ou de rapports.

Exemples : rapports de sauvegarde, alertes système, ...

Serveur d'envoi/réception



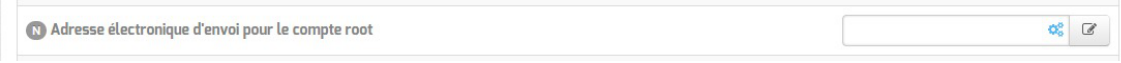
Les paramètres communs à renseigner sont les suivants :

- `Nom de domaine de la messagerie de l'établissement (ex : monetab.ac-aca.fr)`, saisir un nom de domaine valide, par défaut un domaine privé est automatiquement créé avec le préfixe `i-`;
- `Adresse électronique recevant les courriers électroniques à destination du compte root`, permet de configurer une adresse pour recevoir les éventuels messages envoyés par le système.

Le `Nom de domaine de la messagerie de l'établissement` (onglet `Messagerie`) ne peut pas être le même que celui d'un conteneur. Le nom de la machine (onglet `Général`) donne son nom au conteneur maître aussi le `Nom de domaine de la messagerie de l'établissement` ne peut pas avoir la même valeur.

Dans le cas contraire les courriers électroniques utilisant le nom de domaine de la messagerie de l'établissement seront réécris et envoyés à l'adresse électronique d'envoi du compte root.

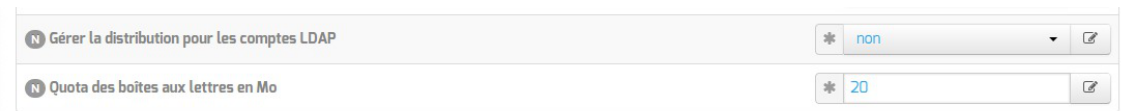
Cette contrainte permet de faire en sorte que les courrier électroniques utilisant un domaine de type `@<NOM CONTENEUR>.*` soit considéré comme des courriers électroniques systèmes.



En mode normal il est possible de configurer le nom de l'émetteur des messages pour le compte `root`.

Certaines passerelles n'acceptent que des adresses de leur domaine.

Toujours en mode normal d'autres paramètres sont modifiables.



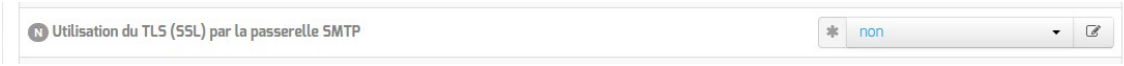
Passer `Gérer la distribution pour les comptes LDAP` à `oui` active les transports LDAP pour la distribution des courriers électroniques, la distribution des courriers locaux est forcée ainsi ils ne sont pas mis en queue et supprimés une semaine plus tard.

Il est également possible de changer la taille des quotas de boîtes aux lettres électroniques qui est fixé par défaut à 20 Mo.

Relai des messages

La variable `Passerelle SMTP`, permet de saisir l'adresse IP ou le nom DNS de la passerelle SMTP à utiliser.

> Afin d'envoyer directement des courriers électroniques sur Internet il est possible de désactiver l'utilisation d'une passerelle en passant `Router les courriels par une passerelle SMTP` à `non`.
>
> Sur les modules possédant un serveur SMTP (Scribe, AmonEcole), ces paramètres sont légèrement différents et des services supplémentaires sont configurables.



`Utilisation du TLS (SSL) par la passerelle SMTP` permet d'activer le support du TLS[p.314] pour l'envoi de message. Si la passerelle SMTP[p.313] accepte le TLS, il faut choisir le port en fonction du support de la commande STARTTLS[p.313] (port 25) ou non (port 465).

2.14. Onglet Authentification : Configuration du proxy authentifié et de FreeRADIUS

EOLE propose un mécanisme d'authentification web via un proxy.

Tous les accès web (HTTP et HTTPS) nécessiteront alors une phase d'authentification.

Cette fonctionnalité offre deux avantages :

- il sera possible de savoir quel utilisateur a accédé à une ressource particulière ;
- il sera possible d'appliquer des politiques de filtrage pour chaque utilisateur.

Pour profiter de cette fonctionnalité, il faut activer l'authentification du proxy dans l'onglet `Authentification` : `Activer l'authentification web (proxy)`.

Cinq méthodes d'authentification sont alors disponibles dans l'onglet `Proxy authentifié`.

Activer une deuxième instance de Squid

Activer une deuxième instance de Squid permet une double authentification, c'est à dire la possibilité de pouvoir configurer deux types distincts d'authentification proxy.

Par exemple, pouvoir utiliser à la fois une authentification NTLM/SMB et une authentification LDAP.

L'implémentation retenue est d'utiliser une instance du logiciel Squid par type d'authentification.

Pour profiter de cette fonctionnalité, il faut passer `Activer une deuxième instance de Squid` à `oui`.

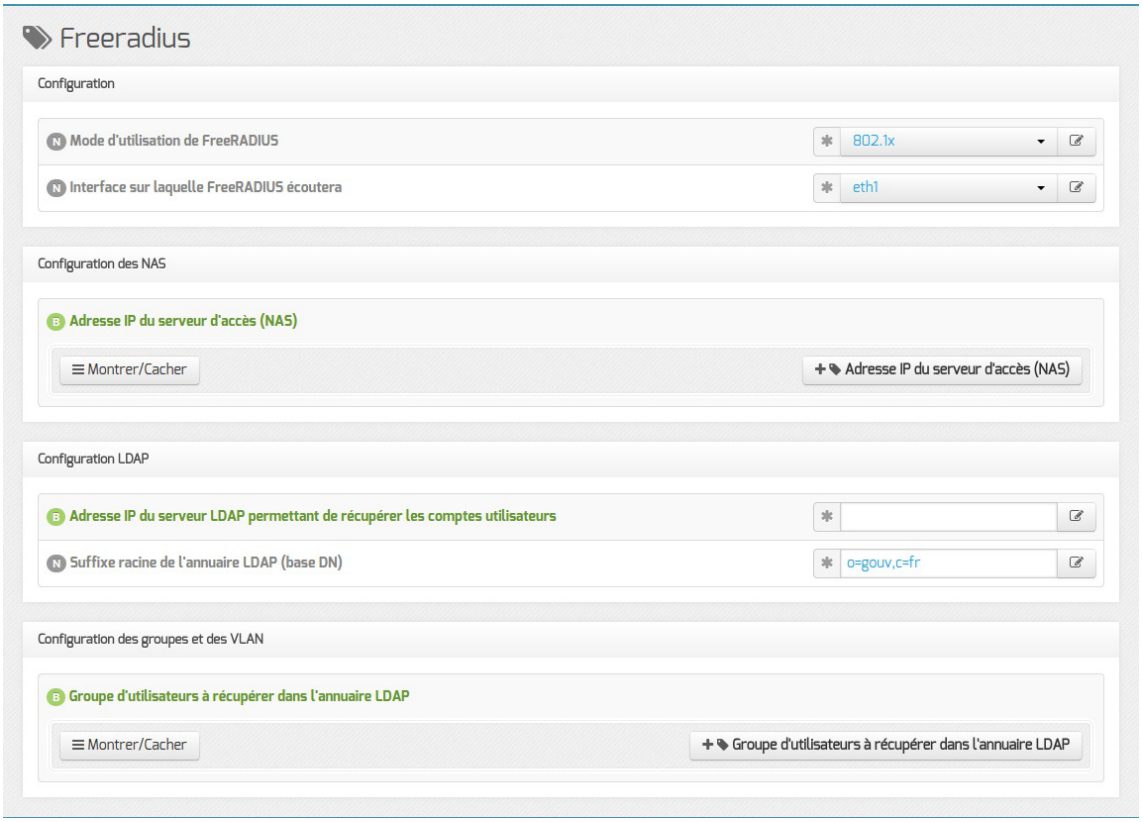
Cela fera apparaître l'onglet `Proxy authentifié 2`.

Activer le service FreeRADIUS

EOLE propose un mécanisme d'authentification réseau basée sur le protocole RADIUS[p.312].

Pour profiter de cette fonctionnalité, il faut activer le service d'authentification RADIUS en passant `Activer le service FreeRADIUS` à `oui`.

Cela fera apparaître l'onglet `Freeradius`.



Vue de l'onglet Freeradius de l'interface de configuration du module

Voir aussi...

- Onglet Proxy authentifié : 5 méthodes d'authentification
- Onglets Proxy authentifié 2 : Double authentification
- Onglet Freeradius : Configuration de l'authentification Radius [p. 85]

2.15. Onglet Proxy authentifié : 5 méthodes d'authentification

EOLE propose un mécanisme d'authentification web via un proxy.

Tous les accès web (HTTP et HTTPS) nécessiteront alors une phase d'authentification.

Cette fonctionnalité offre deux avantages :

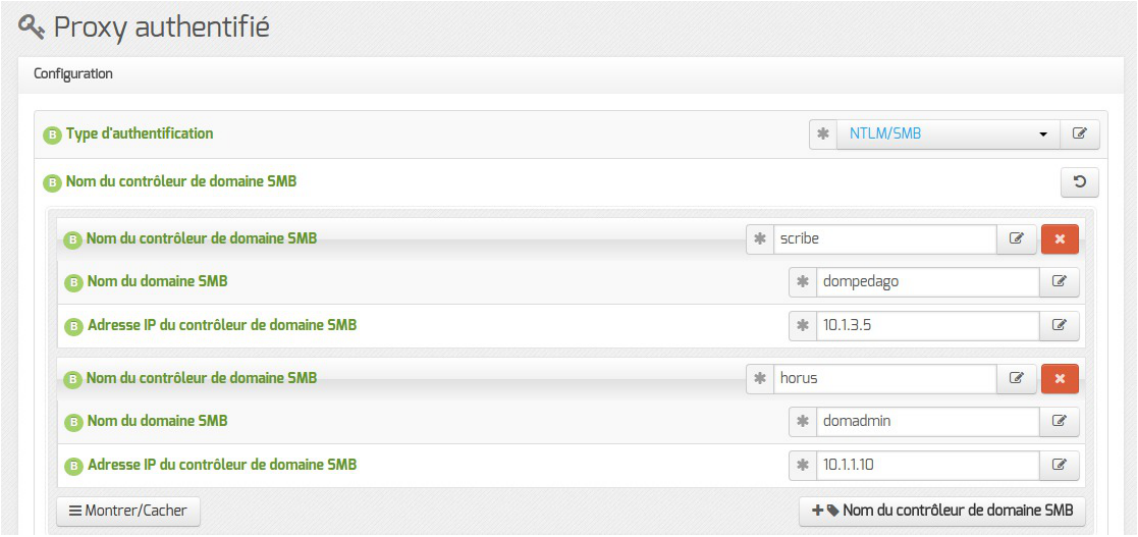
- il sera possible de savoir quel utilisateur a accédé à une ressource particulière ;
- il sera possible d'appliquer des politiques de filtrage pour chaque utilisateur.

Pour profiter de cette fonctionnalité, il faut activer l'authentification du proxy dans l'onglet `Authentification` : `Activer l'authentification web (proxy)`.

Cinq méthodes d'authentification sont alors disponibles dans l'onglet `Proxy authentifié`.

Authentification NTLM/SMB

Il s'agit d'une authentification transparente pour les postes utilisateurs Windows intégrés dans un domaine Samba.



Il est possible de configurer plusieurs contrôleurs de domaine dans le cadre de l'authentification NTLM/SMB.

C'est la configuration à choisir si vous disposez d'un serveur pédagogique Scribe et/ou d'un serveur administratif Horus.

La syntaxe pour utiliser le proxy authentifié avec une machine hors domaine est `domaine\login` mais elle ne fonctionne pas avec toutes les versions de navigateurs.

L'authentification NTLM/SMB nécessite l'application de la clé de registre suivante sur les clients Windows Vista et Windows Seven :

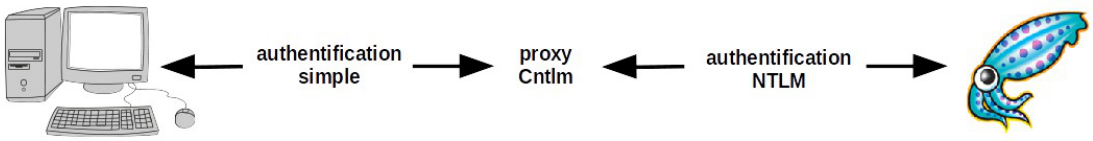
```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa]
"LMCompatibilityLevel"=dword:00000001
```

Pour plus d'informations, consulter : http://technet.microsoft.com/en-us/library/cc960646

Authentification NTLM/SMB poste hors domaine

En mode normal, l'authentification NTLM[p.309] peut être facilitée par l'utilisation d'un proxy. Le proxy NTLM proposé par EOLE utilise le logiciel libre Cntlm[p.303].

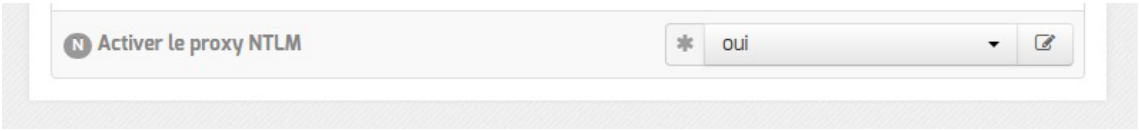
Le proxy NTLM Cntlm est pré-installé sur les modules Amon, AmonEcole et ses variantes.



Cette méthode permet d'utiliser l'authentification NTLM sur des machines qui ne savent pas le gérer. Ce

qui est le cas des machines hors domaine.

Pour activer le proxy NTLM Cntlm il faut passer la variable `Activer le proxy NTLM` à `oui`.



Le port utilisé par défaut par Cntlm est `3127`, il est modifiable en mode expert.

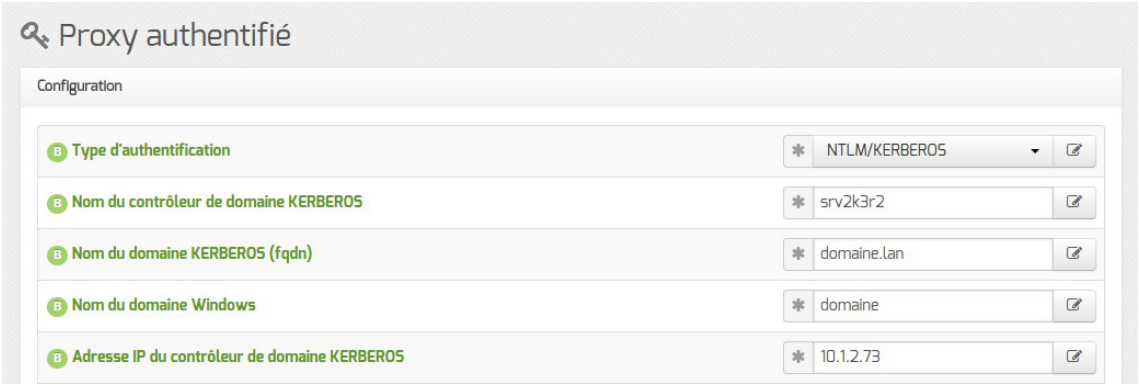
Pour continuer à profiter de l'authentification transparente, les postes intégrés au domaine ne doivent pas passer par Cntlm.

Les postes intégrés au domaine doivent donc utiliser le port `3128` pour passer par le proxy et les postes nomades (hors domaine) doivent utiliser le port `3127` pour passer par Cntlm.

Dans le cas où la découverte automatique du proxy avec WPAD est activée, le port proposé par défaut est automatiquement celui du proxy NTLM Cntlm (`3127` par défaut).

C'est le premier domaine spécifié qui sera utilisé par Cntlm.

Authentification NTLM/KERBEROS



Il s'agit d'une authentification transparente pour les postes utilisateurs Windows intégrés dans un domaine Active Directory.

Cette méthode d'authentification nécessite l'intégration du serveur au royaume Kerberos.

L'intégration peut être réalisée lors de l'instanciation du module en répondant `oui` à la question suivante :

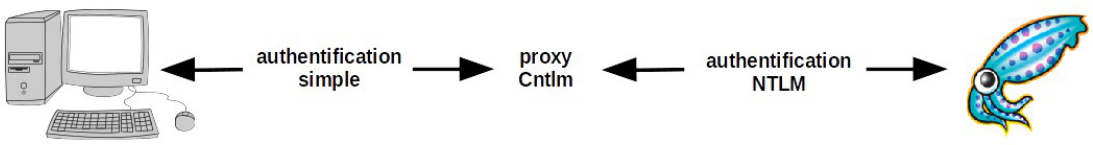
```
Voulez-vous (ré)intégrer le serveur au domaine maintenant ?
```

Si la configuration de l'authentification NTLM/KERBEROS est réalisée après l'instanciation, il est possible de relancer l'intégration du serveur à tout moment à l'aide du script `enregistrement_domaine.sh`.

Authentification NTLM/KERBEROS poste hors domaine

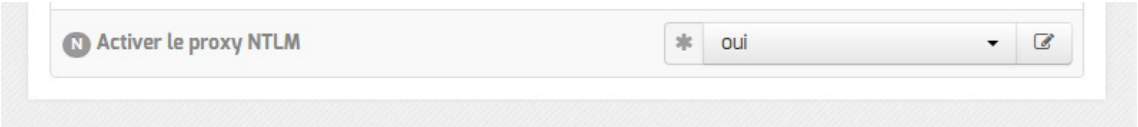
En mode normal, l'authentification NTLM[p.309] peut être facilitée par l'utilisation d'un proxy. Le proxy NTLM proposé par EOLE utilise le logiciel libre Cntlm[p.303].

Le proxy NTLM Cntlm est pré-installé sur les modules Amon, AmonEcole et ses variantes.



Cette méthode permet d'utiliser l'authentification NTLM sur des machines qui ne savent pas le gérer. Ce qui est le cas des machines hors domaine.

Pour activer le proxy NTLM Cntlm il faut passer la variable `Activer le proxy NTLM` à `oui`.



Le port utilisé par défaut par Cntlm est `3127`, il est modifiable en mode expert.

Pour continuer à profiter de l'authentification transparente, les postes intégrés au domaine ne doivent pas passer par Cntlm.

Les postes intégrés au domaine doivent donc utiliser le port `3128` pour passer par le proxy et les postes nomades (hors domaine) doivent utiliser le port `3127` pour passer par Cntlm.

Dans le cas où la découverte automatique du proxy avec WPAD est activée, le port proposé par défaut est automatiquement celui du proxy NTLM Cntlm (`3127` par défaut).

Authentification LDAP

Il s'agit d'une authentification non transparente s'appuyant sur un annuaire de type OpenLDAP.

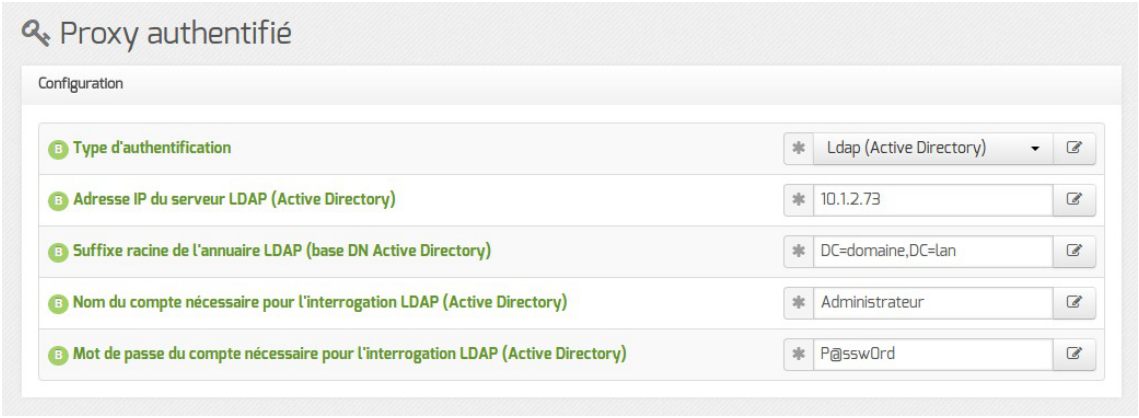
Ce type d'authentification est recommandé pour les postes hors domaine.

En mode normal, il est possible de déclarer un annuaire de secours.

Cet annuaire est interrogé uniquement si le premier ne répond pas.

Cette fonctionnalité est recommandée dans le cas d'annuaires répliqués.

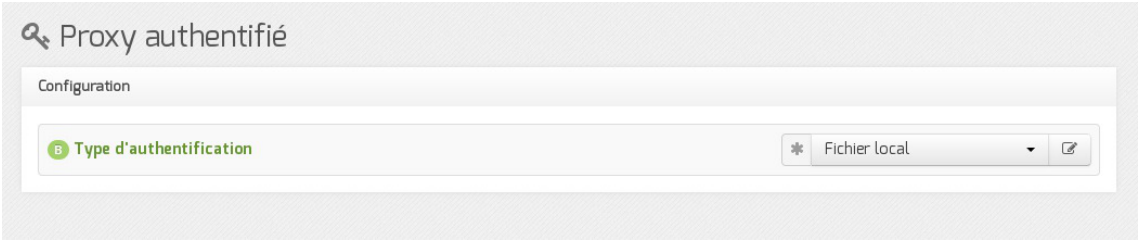
Authentification LDAP (Active Directory)



Il s'agit d'une authentification non transparente s'appuyant sur un annuaire de type Active Directory.

Ce type d'authentification est recommandé pour les postes hors domaine.

Authentification sur Fichier local



Il s'agit d'une authentification non transparente s'appuyant sur un fichier de comptes locaux.

Ce type d'authentification peut être utilisé dans une petite structure, comme une école, qui ne disposerait pas vraiment d'un réseau local.

Pour cette authentification, le fichier utilisé par défaut est : `/etc/squid3/users`

Il doit être au format *htpasswd* et il peut être peuplé en utilisant la commande suivante :

```
# htpasswd -c /etc/squid3/users <compte>
```

En mode conteneur (module AmonEcole par exemple), le fichier `/etc/squid3/users` se trouve dans le conteneur `proxy` :

```
# ssh proxy
# htpasswd -c /etc/squid3/users <compte>
```

ou

```
# CreoleRun "htpasswd -c /etc/squid3/users <compte>" proxy
```

Désactivation de l'authentification sur une interface

Pour chacune des interfaces (hors eth0 si plusieurs interfaces sont configurées), il est possible d'activer/désactiver l'authentification proxy.

Par exemple, pour désactiver l'authentification proxy uniquement sur le réseau eth2, il faut aller dans

l'onglet `Interface-2` et répondre `non` à la question `Activer l'authentification sur cette interface (s'applique aussi aux VLAN)`.

2.16. Onglets Proxy authentifié 2 : Double authentification

Par double authentification, nous entendons la possibilité de pouvoir configurer deux types distincts d'authentification proxy.

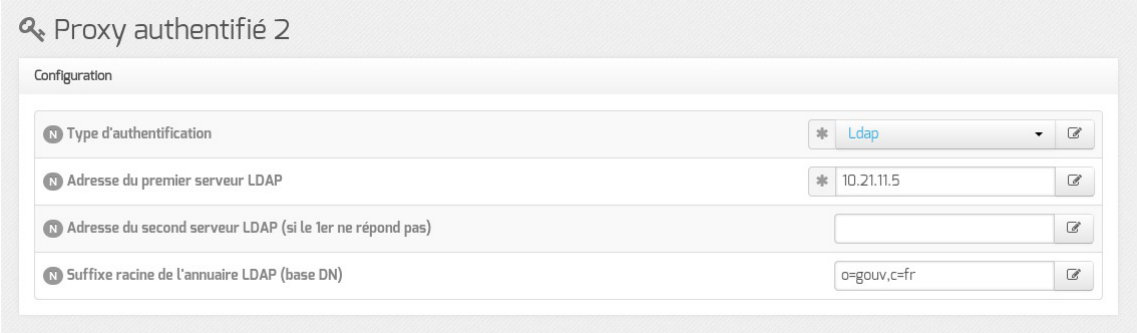
Par exemple, pouvoir utiliser à la fois une authentification NTLM/SMB et une authentification LDAP.

L'implémentation retenue est d'utiliser une instance du logiciel Squid par type d'authentification.

Configuration pas à pas

1. Activation de la deuxième instance de Squid dans l'onglet `Authentification` :

2. Configuration du type d'authentification dans l'onglet `Proxy authentifié 2` :



Notes techniques

Les fichiers de logs spécifiques au second type d'authentifications sont les suivants :

- `/var/log/rsyslog/local/squid/squid2.info.log`
- `/var/log/rsyslog/local/e2guardian/e2guardian2.info.log`

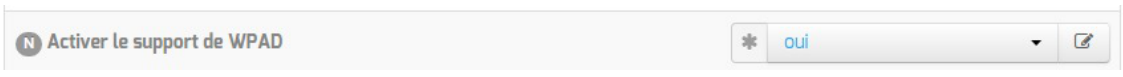
Dans l'état actuel, ces logs ne sont pas consultables au travers de l'interface EAD et seule la première configuration proxy est distribuée par WPAD (voir partie dédiée).

2.17. Onglet Wpad : découverte automatique du proxy

WPAD est mise à disposition sur les modules Amon et ses variantes (AmonEcole, ...) au travers du paquet `eole-wpad` mais n'est fonctionnel que si le paquet `eole-proxy` est installé.

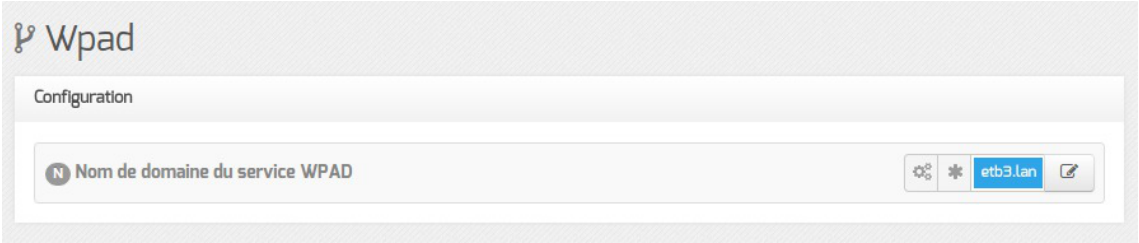
Pour fonctionner correctement, il faut que l'URL `wpad.<nom domaine local>` correspondre à l'adresse IP du serveur web.

Le support de WPAD doit être activé et correctement configuré sur le module Amon.



Activation de WPAD dans l'onglet Services

Dans l'onglet `Services` de l'interface de configuration du module `Activer le support de WPAD` doit être placé à `oui`.



Vue de l'onglet Wpad dans l'interface de configuration du module

Cela rend disponible l'onglet `Wpad` au sein duquel le `Nom de domaine du service WPAD` doit être rempli avec la même valeur que le `Nom de domaine privé du réseau local` présent dans l'onglet `Général`.

Si vous souhaitez utiliser un autre nom de domaine qui ne correspondrait pas au `Nom de domaine privé du réseau local` de l'onglet `Général`, il faut le déclarer dans le champ `Nom domaine local supplémentaire ou rien` de l'onglet `Zones-dns`.

Pour être pris en compte, les changements doivent être enregistrés et suivis de la commande `reconfigure` sur le module.

WPAD supporte les VLAN et les alias, Nginx renvoie le bon fichier WPAD si des VLAN ou des alias sont déclarés.

En mode expert, Il est également possible de changer le port du proxy diffusé par défaut pour une interface, un VLAN ou un alias donné.

Voir aussi...

Configurer la découverte automatique du proxy avec WPAD [p.197]

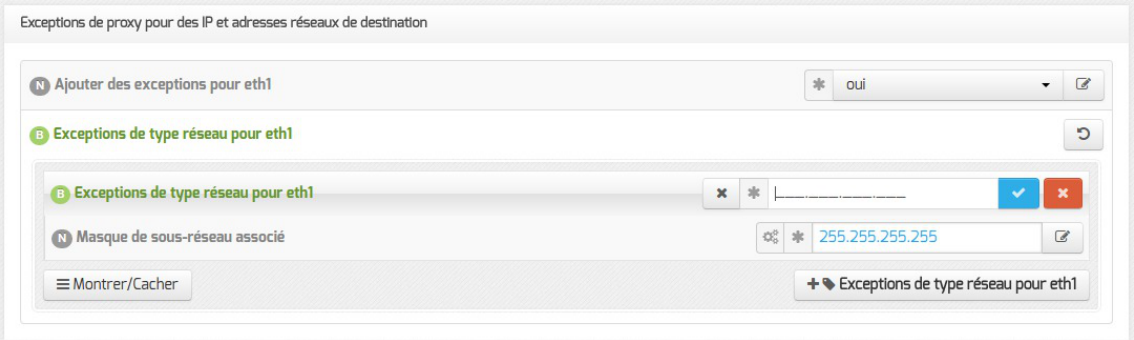
2.18. Onglet Exceptions proxy

Dans l'onglet `Exceptions proxy` de l'interface de configuration du module il est possible d'ajouter des exclusions dans la configuration automatique du proxy.

Il est possible de déclarer différents types d'exceptions.

Exception sur une adresse IP ou une plage d'adresses IP

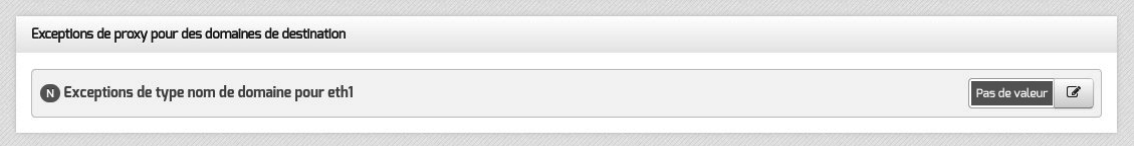
Cette exception commune à ERA et à WPAD permet de déclarer une adresse IP ou une plage d'adresses IP de destination pour laquelle on ne passe pas par le proxy.



Le bouton `Exceptions de type réseau pour eth-n` permet d'ajouter plusieurs exceptions sur une même interface.

Exception sur un nom de domaine

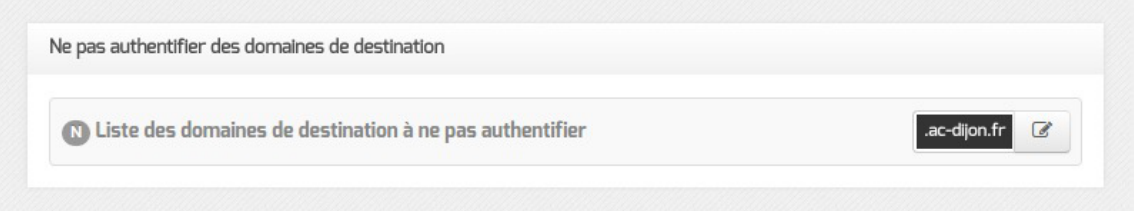
Cette exception commune à ERA et à WPAD permet de déclarer un domaine de destination pour lequelle on ne passe pas par le proxy.



Il est possible d'ajouter plusieurs exceptions sur une même interface.

Exception au niveau de l'authentification des domaines

Cette exception permet de déclarer des sites pour lesquels le proxy ne demandera pas l'authentification à l'utilisateur qui souhaite y accéder.



Si cNTLM et WPAD sur activés sur l'interface réseau, les utilisateurs utiliseront directement Squid (sans passer par cNTLM) pour accéder à ces sites.

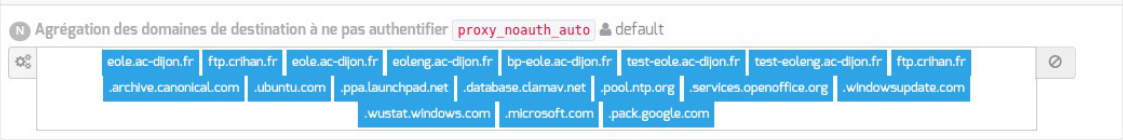
Les domaines commençants par un `.` sont gérés, le domaine lui-même et les sous-domaines ne sont pas authentifiés.

Si on spécifie la valeur `.ac-dijon.fr` alors `ac-dijon.fr` et `www.ac-dijon.fr` seront autorisés sans authentification.

Une liste de sites à ne pas authentifier par défaut est stockée dans la variable cachée `proxy noauth auto`.

Il est possible de l'afficher dans l'onglet `Exceptions proxy` de l'interface de configuration du

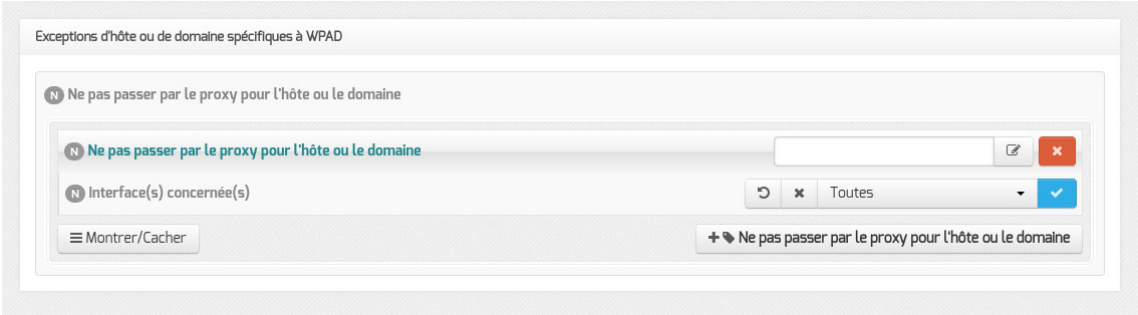
module en activant le mode Debug.



Cette variable reprend la liste des sites qui étaient dans le template `domaines_noauth` des versions EOLE antérieures à 2.5.2.

Exception sur un nom d'hôte (spécifique à WPAD)

L'exception sur un nom d'hôte s'effectue sur le nom d'hôte et sur le nom d'hôte complet.



Il faut choisir une interface ou toutes les interfaces sur lesquelles l'exception sera appliquée. Le bouton `+ Ne pas passer par le proxy pour l'hôte ou le domaine` permet d'ajouter plusieurs exceptions sur une même interface.

Ce type d'exception étant spécifique à WPAD, il n'est pas prise en compte par les autres services gérant des exceptions au niveau du proxy.

Si le champ `Ne pas passer par le proxy pour l'hôte ou le domaine` a comme valeur `www.ac-monacad.fr`, le fichier WPAD.dat généré contiendra la ligne `|| localHostOrDomainIs(host, "www.ac-monacad.fr")` qui permet d'exclure simplement des URLs.

Compléments sur `Ne pas passer par le proxy pour le domaine` (dnsDomainIs) :

http://findproxyforurl.com/netscape-documentation/#dnsDomainIs

Compléments sur `Ne pas passer par le proxy pour l'hôte ou le domaine` (localHostOrDomainIs) :

http://findproxyforurl.com/netscape-documentation/#localHostOrDomainIs

2.19. Onglet Reverse proxy : Configuration du proxy inverse

EOLE propose un serveur proxy inverse (reverse proxy) basé sur le logiciel libre Nginx[p.308].

Le proxy inverse est un type de serveur proxy, habituellement placé en frontal de serveurs web, qui permet de relayer des requêtes web provenant de l'extérieur vers les serveurs internes (situés en DMZ[p.

304] par exemple). Cela le différencie grandement d'un proxy classique comme Squid[p.313].

Concrètement, le proxy inverse permet d'ouvrir des services web installés sur des serveurs situées "derrière" le pare-feu l'accès sur Internet sans avoir recours à des règles *iptables/DNAT*.

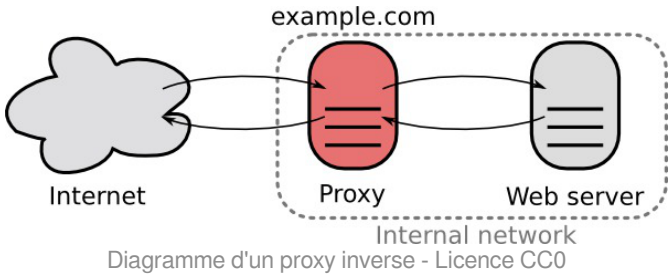
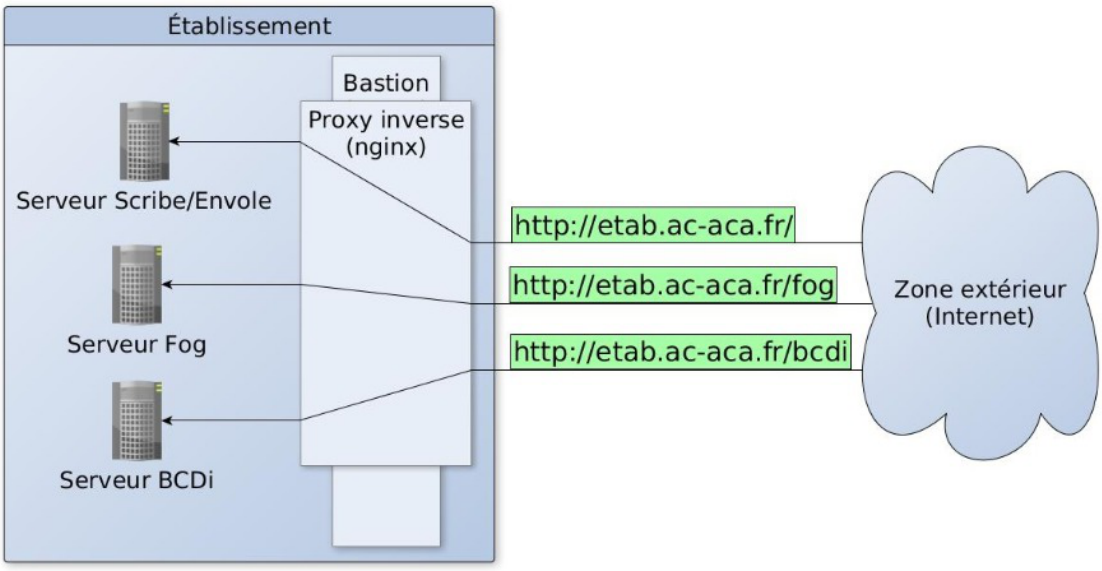


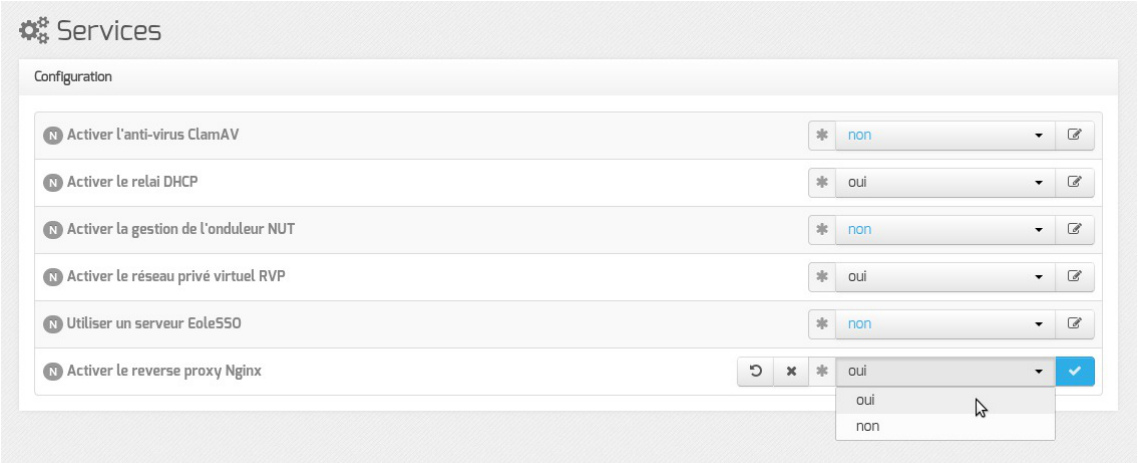
Diagramme d'un proxy inverse - Licence CC0

Le proxy inverse EOLE peut relayer des requêtes vers les services suivants :

- les serveurs EoleSSO ;
- les EAD ;
- le serveur d'administration d'Envole ;
- le protocole HTTP[p.306] ;
- le protocole HTTPS[p.306].



Avant toute chose, le proxy inverse doit être activé dans l'onglet `Services` en passant `Activer le reverse proxy Nginx` à `oui`.



Vue de l'onglet Services de l'interface de configuration du module

L'activation du service fait apparaître un nouvel onglet.

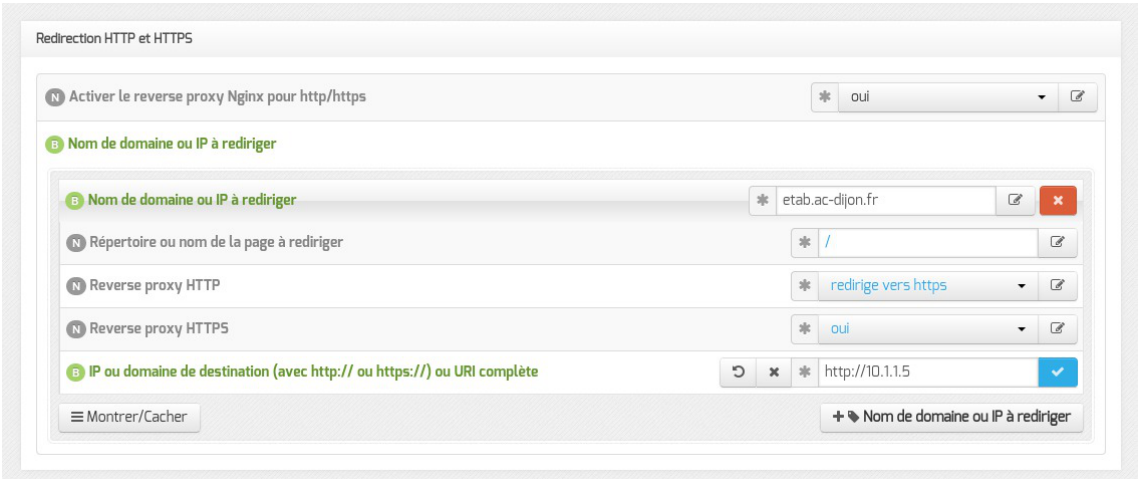
Vue de l'onglet Reverse proxy de l'interface de configuration du module

Redirection de services particuliers

Pour rediriger le service EoleSSO (port 8443) il faut indiquer l'adresse IP ou le nom de domaine interne de la machine de destination (adresse IP ou le nom de domaine interne du module Scribe). Si le service EoleSSO est activé localement il est impossible de réaliser une redirection pour ce service.

Le service SSO local du module Amon ne devra pas être activé si vous renseignez l'adresse d'un service SSO distant au niveau du proxy inverse.

Redirection HTTP et HTTPS

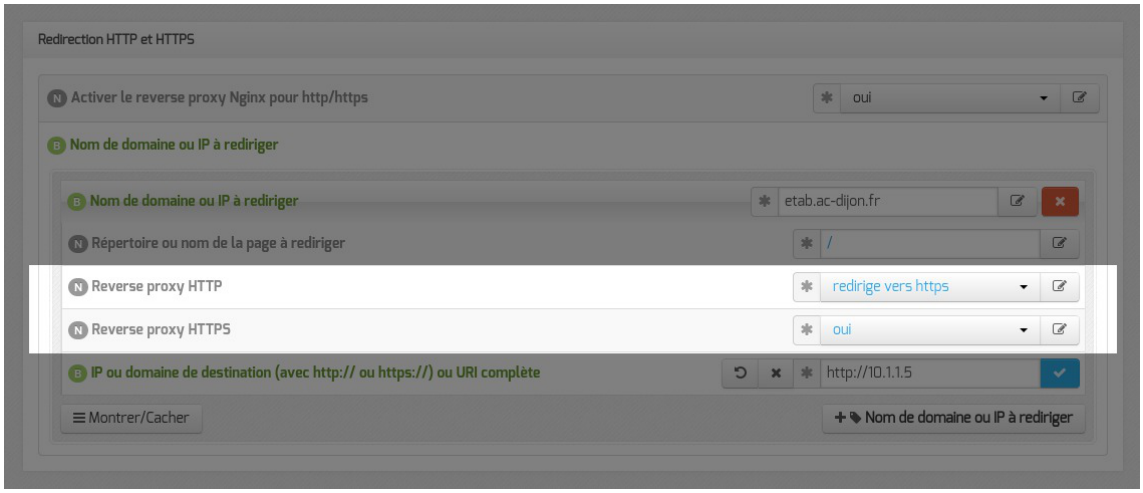


Pour rediriger HTTP et HTTPS il est nécessaire de passer la variable `Activer le reverse proxy Nginx pour le http/https` à `oui` et de renseigner plus d'informations :

- le `Nom de domaine ou IP à rediriger` : le nom de domaine diffusé auprès des utilisateurs.

Ce nom de domaine est celui qui permet d'accéder au module Amon ou AmonEcole ;

- le `Répertoire ou nom de la page à rediriger` permet de rediriger un sous-répertoire vers une machine. La valeur par défaut est `/` ;
- l'`IP ou domaine de destination (avec http:// ou https://) ou URI complète` permet de saisir l'adresse IP (exemple : `http://192.168.10.1`), le nom de domaine (exemple : `http://scribe.monetab.fr`) ou l'URI[p.314] (exemple : `http://scribe.monetab.fr/webmail/`) du serveur de destination hébergeant la ou les applications.



Il est possible de forcer l'utilisation du protocole HTTPS pour les requêtes utilisant le protocole HTTP de façon transparente. De cette manière, un utilisateur web se connectant à l'adresse `http://monetab.fr` sera automatiquement redirigé vers `https://monetab.fr`

Ainsi les communications sont automatiquement chiffrées protégeant la transmission de données sensibles (nom d'utilisateur, mot de passe, etc.).

Le proxy inverse peut être utilisé pour ne rediriger que le HTTPS en passant les valeurs `Reverse proxy HTTP` à `non` et `Reverse proxy HTTPS` à `oui`.

Il est possible d'ajouter plusieurs redirections en cliquant sur le bouton `Nom de domaine ou IP à rediriger`.

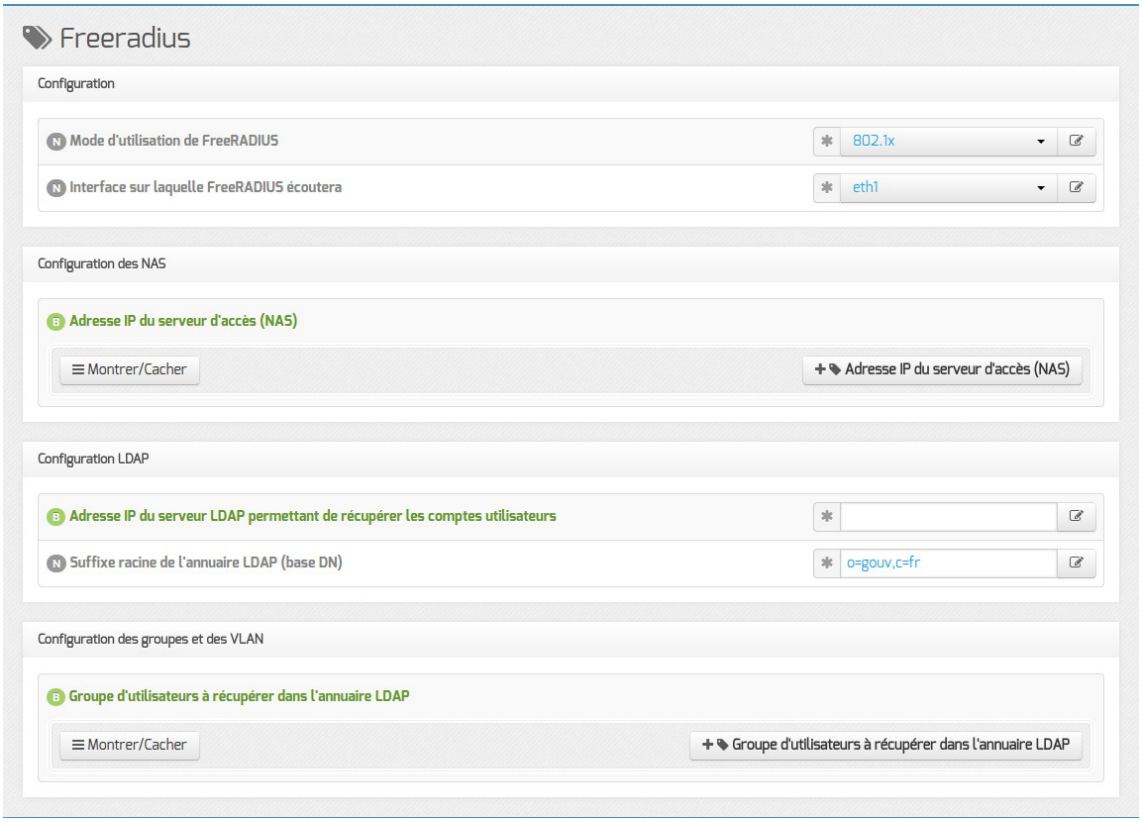
Un répertoire déterminé peut également être redirigé vers un serveur différent. Par exemple le lien vers l'application Pronote[p.311], `https://monetab.fr/pronote/` peut être redirigé vers `http://pronote.monetab.fr/` (attention, le "/" final est important, puisqu'il faut rediriger à la racine du serveur de destination).

2.20. Onglet Freeradius : Configuration de l'authentification Radius

EOLE propose un mécanisme d'authentification réseau basé sur le protocole RADIUS[p.312].

Pour profiter de cette fonctionnalité, il faut activer le service d'authentification RADIUS en passant `Activer le service FreeRADIUS` à `oui` dans l'onglet `Authentification`.

Cela fera apparaître l'onglet `Freeradius`.



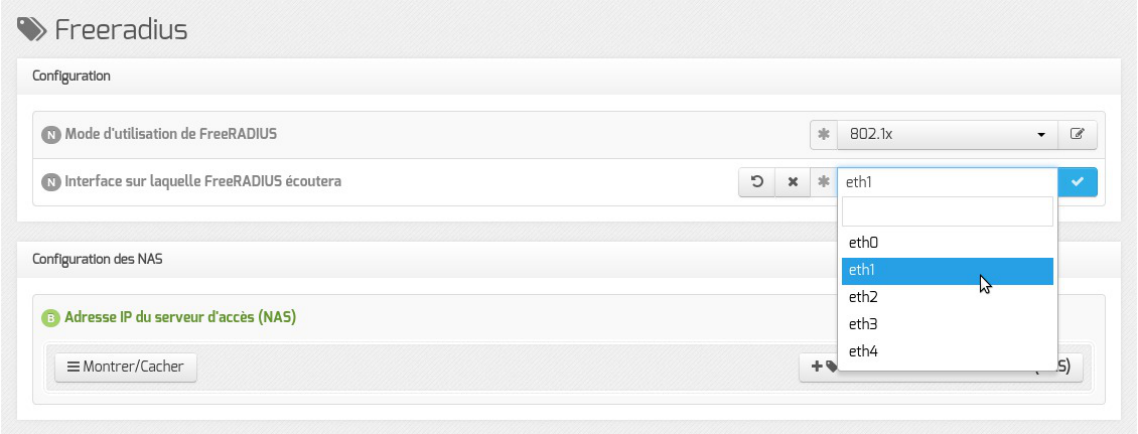
Vue de l'onglet Freeradius de l'interface de configuration du module

Il est possible de choisir entre 2 modes d'utilisation de FreeRADIUS :

- 802.1x ;
- accounting.

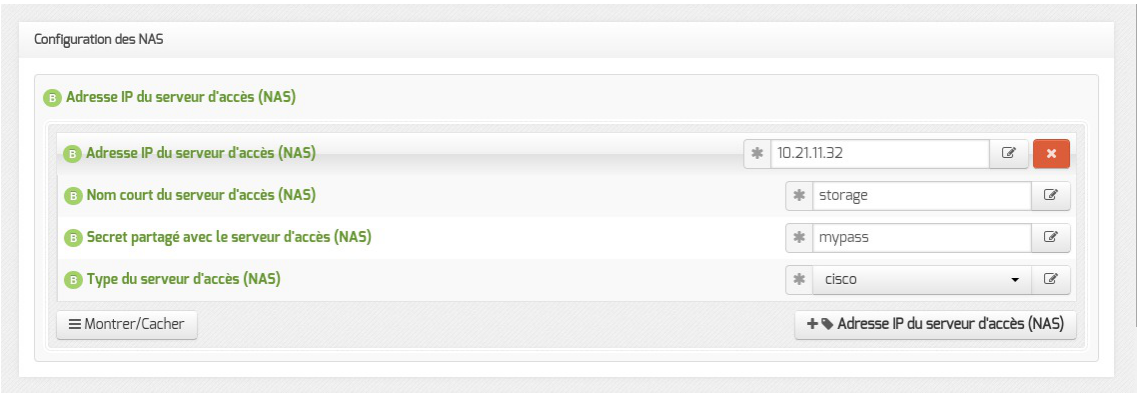
Le mode 802.1x

Le mode `802.1x` permet de taguer dynamiquement des ports d'un switch (NAS[p.308]) sur lesquels sont brassées des stations en fonction du compte LDAP de connexion.



`Interface sur laquelle FreeRADIUS écoutera` : définition de l'interface d'écoute de FreeRADIUS.

Configuration des NAS



`Adresse IP du serveur d'accès (NAS)` : adresse IP du switch.

`Nom court du serveur d'accès (NAS)` : libellé du switch.

`Secret partagé avec le serveur d'accès (NAS)` : secret partagé entre FreeRADIUS et le switch.

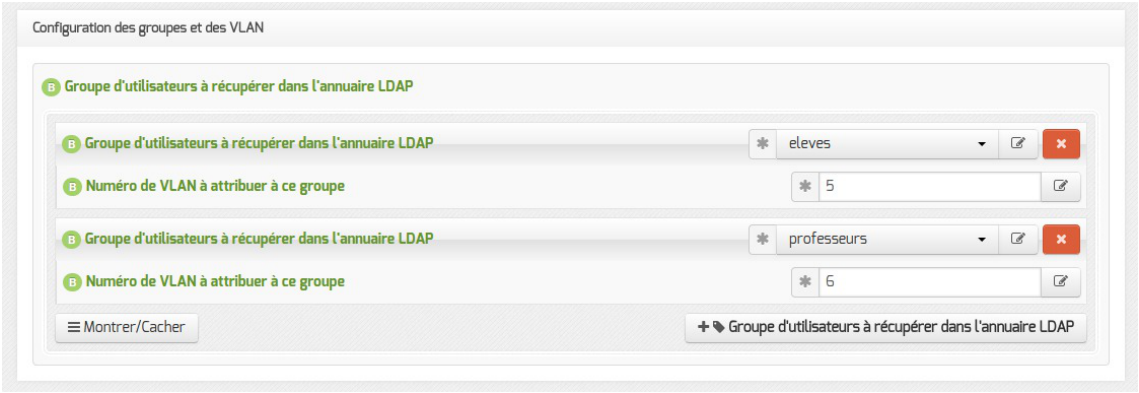
`Type du serveur d'accès (NAS)` : type de switch.

Configuration LDAP

`Adresse IP du serveur LDAP permettant de récupérer les comptes utilisateurs` : adresse IP LDAP.

`Suffixe racine de l'annuaire LDAP (base DN)` : *ou=education,o=gouv,c=fr* par exemple.

Configuration des groupes et des VLAN



`Groupe d'utilisateurs à récupérer dans l'annuaire LDAP` : saisir ou choisir un groupe existant dans l'annuaire.

`Numéro de VLAN à attribuer à ce groupe` : les machines se connectant avec un utilisateur appartenant au groupe indiqué ci-dessus verra son port tagué sur ce numéro de VLAN.

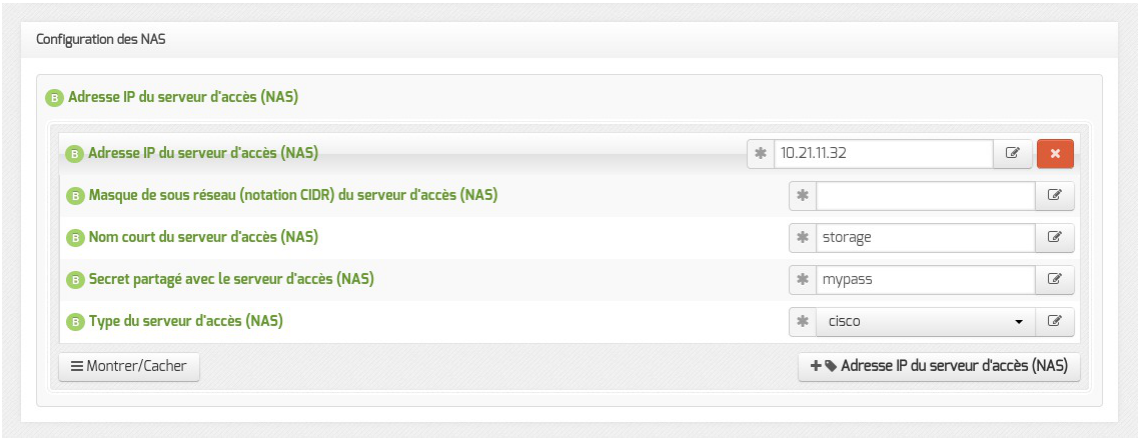
Le mode accounting

Le mode accounting permet de créer un réseau Wi-Fi WPA enterprise sur une borne Wi-Fi (NAS) ayant pour identifiants autorisés les compte/motDePasse de l'annuaire LDAP déclaré.

Onglet Freeradius - mode accounting

`Adresse IP sur laquelle FreeRADIUS écoutera` : l'adresse IP d'une des interfaces du serveur.

Configuration des NAS



Onglet Freeradius - mode accounting

`Adresse IP du serveur d'accès (NAS)` : adresse IP de la borne Wi-Fi.

`Masque de sous réseau (notation CIDR) du serveur d'accès (NAS)` : 24 (en notation

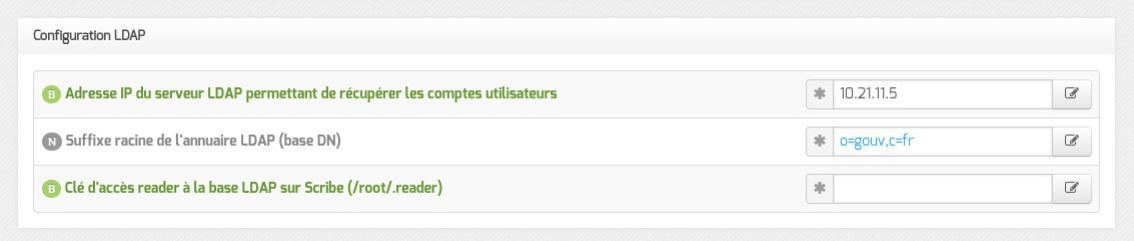
CIDR[p.302]) si le réseau est de classe C.

`Nom court du serveur d'accès (NAS)` : libellé de la borne Wi-Fi.

`Secret partagé avec le serveur d'accès (NAS)` : secret partagé entre FreeRADIUS et la borne Wi-Fi.

`Type du serveur d'accès (NAS)` : type de borne (other en général).

Configuration LDAP



Onglet Freeradius - mode accounting

`Adresse IP du serveur LDAP permettant de récupérer les comptes utilisateurs` : adresse IP ldap.

`Suffixe racine de l'annuaire LDAP (base DN)` : *ou=education,o=gouv,c=fr* par exemple.

`Clé d'accès reader à la base ldap sur Scribe (/root/.reader)` : à récupérer sur le serveur LDAP.

3. Configuration en mode expert

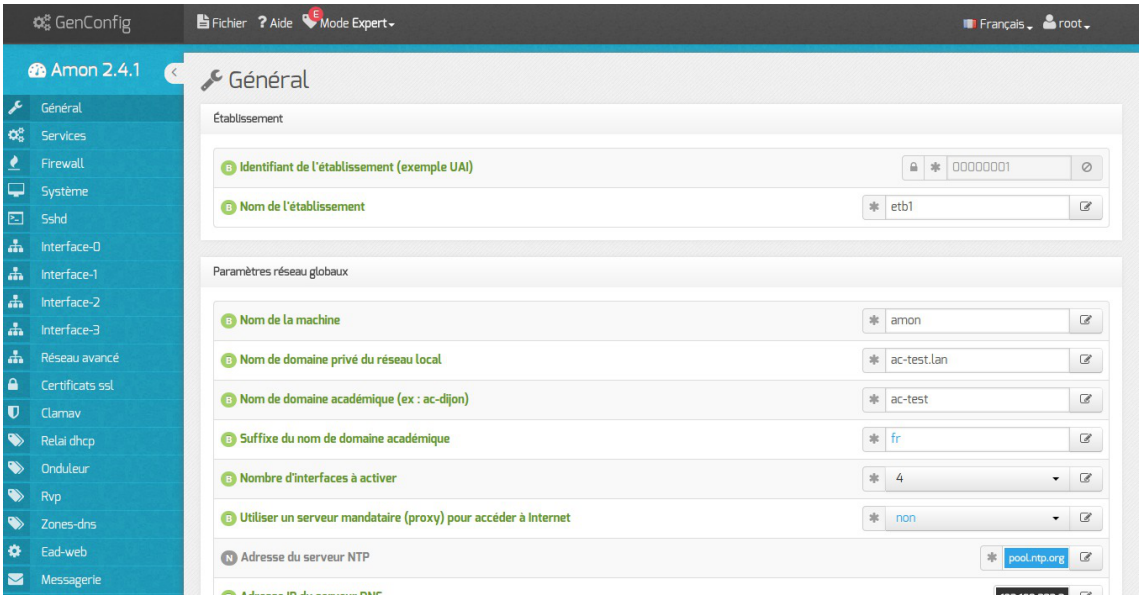
Certains onglets et certaines options ne sont disponibles qu'après avoir activé le mode expert de l'interface de configuration du module.

Dans l'interface de configuration du module voici les onglets propres à la configuration du module Amon :

- `Général` ;
- `Services` ;
- `Firewall` ;
- `Système` ;
- `Sshd` ;
- `Logs` * ;
- `Interface-0` (configuration de l'interface réseau) ;
- `Interface-1` (configuration de l'interface réseau) ;
- `Réseau avancé` ;
- `Certificat ssl` ;
- `Agregation` ** ;
- `Clamav` * ;
- `Relai dhcp` * ;

- Onduleur * ;
- Eole sso * ;
- Rvp * ;
- Zone-dns ;
- Ead-web ;
- Messagerie ;
- Authentification ;
- Filtrage web ;
- Squid ;
- Squid2 **;
- Proxy authentifié ;
- Proxy authentifié 2 **;
- Wpad ;
- Exceptions proxy ;
- Proxy parent ;
- Reverse proxy * ;
- Freeradius **;
- Eoleflask.

Certains des onglets ne sont disponibles qu'après activation du service dans l'onglet Services et sont marqués avec une * dans la liste ci-dessus.



Vue générale de l'interface de configuration du module

Dans les onglets Général et Firewall, deux options sont à renseigner avec la plus grande attention : le `Nombre d'interfaces à activer` et le `Modèle de filtrage`.

En effet, ces options vont orienter l'architecture de vos réseaux internes ainsi qu'une partie importante de la politique de sécurité qui sera mise en place.

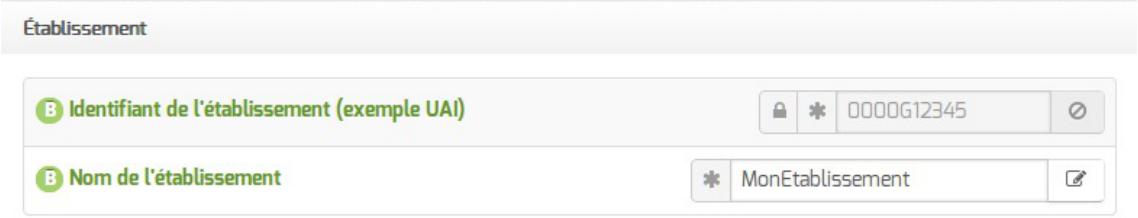
Le nombre d'interfaces doit, bien évidemment, être choisi en fonction du nombre de cartes réseau physiques du serveur mais plus encore en fonction du nombre de sous-réseaux souhaités.

Le modèle de filtrage doit être choisi en fonction du nombre d'interfaces activées et des services que l'on souhaite mettre en place.

3.1. Onglet Général

Présentation des différents paramètres de l'onglet `Général`.

Informations sur l'établissement



Deux informations sont importantes pour l'établissement :

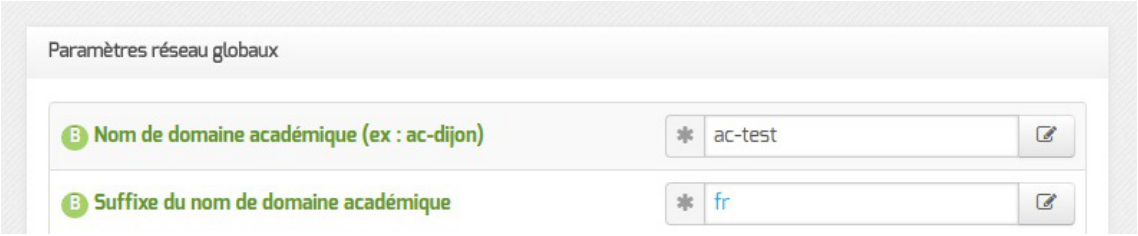
- l'`Identifiant de l'établissement`, qui doit être unique ;
- le `Nom de l'établissement`.

Ces informations sont notamment utiles pour Zéphir, les applications web locales, ...

Sur les modules fournissant un annuaire LDAP[p.307] local, ces variables sont utilisées pour créer l'arborescence.

Il est déconseillé de modifier ces informations après l'instanciation du serveur sur les modules utilisant un serveur LDAP local.

Paramètres réseau globaux



En premier lieu, il convient de configurer les noms de domaine de la machine.

Cette information est découpée en plusieurs champs :

- le nom de la machine dans l'établissement ;
- le nom du domaine privé utilisé à l'intérieur de l'établissement ;
- le nom de domaine académique et son suffixe.

Le `Nom de la machine` est laissé à l'appréciation de l'administrateur.

Les domaines de premier niveau `.com`, `.fr` sont en vigueur sur Internet, mais sont le résultat d'un choix arbitraire.

Sur un réseau local les noms de domaine sont privés et on peut tout à fait utiliser des domaines de premier niveau, et leur donner la sémantique que l'on veut.

Le `Nom de domaine privé du réseau local` utilise fréquemment des domaines de premier niveau du type `.lan` ou `.local`.

C'est ce nom qui configurera le serveur DNS (sur un module Amon par exemple) comme zone de résolution par défaut. Il sera utilisé par les machines pour résoudre l'ensemble des adresses locales.

Les informations sur les noms de domaine sont importantes car elles sont notamment utilisées pour l'envoi des courriels et pour la création de l'arborescence de l'annuaire LDAP.

L'usage d'un domaine de premier niveau utilisé sur Internet n'est pas recommandé, car il existe un risque de collision entre le domaine privé et le domaine public.

Nombre d'interfaces

Un module Amon peut avoir de 2 à 5 cartes réseau.

Le nombre d'interfaces activées se définit dans l'onglet `Général` de l'interface de configuration du module.

Cela ajoute autant d'onglets `Interface-n` que le nombre d'interfaces à activer choisi.

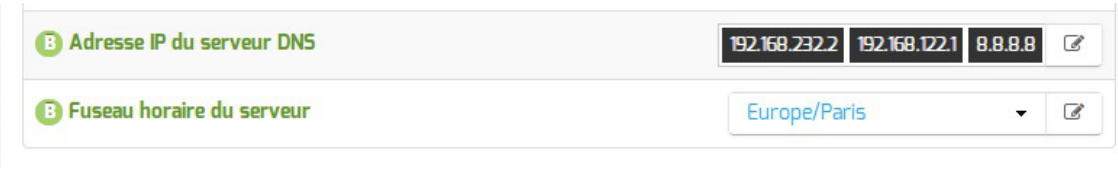
Proxy

Si le module doit utiliser un proxy pour accéder à Internet, il faut activer cette fonctionnalité en passant la variable `Utiliser un serveur mandataire (proxy) pour accéder à Internet` à `oui`.

Il devient alors possible de saisir la configuration du serveur proxy :

- nom de domaine ou adresse IP du serveur proxy ;
- le port du proxy.

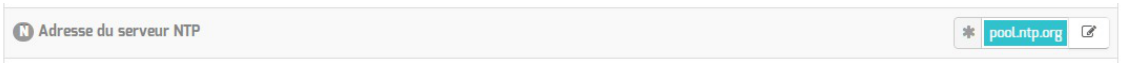
DNS et fuseau horaire



La variable `Adresse IP du serveur DNS` donne la possibilité de saisir une ou plusieurs adresses IP du ou des serveur(s) de noms DNS[p.304].

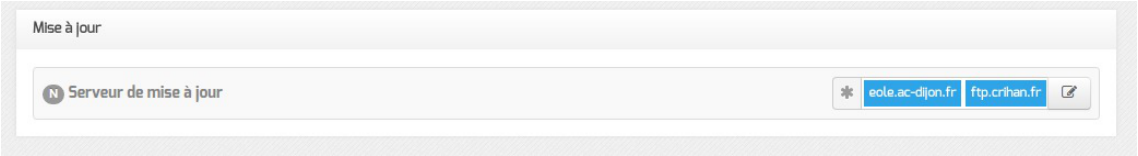
La variable `Fuseau horaire du serveur` vous permet de choisir votre fuseau horaire dans une liste conséquente de propositions.

NTP

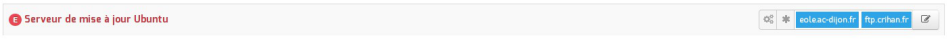


Une valeur par défaut est attribuée pour le serveur de temps NTP[p.309]. Il est possible de changer cette valeur pour utiliser un serveur de temps personnalisé.

Mise à jour



Il est possible de définir une autre adresse pour le serveur de mise à jour EOLE que celle fournie par défaut, dans le cas où vous auriez, par exemple, un miroir des dépôts.



Il est possible de définir d'autres adresses pour le serveur de mise à jour Ubuntu que celles fournies par défaut, dans le cas où vous auriez, par exemple, un miroir des dépôts.

Le champ `Adresse web de mise à jour des blacklists` permet de personnaliser l'adresse à utiliser pour le téléchargement des bases de filtres (blacklists[p.307]).

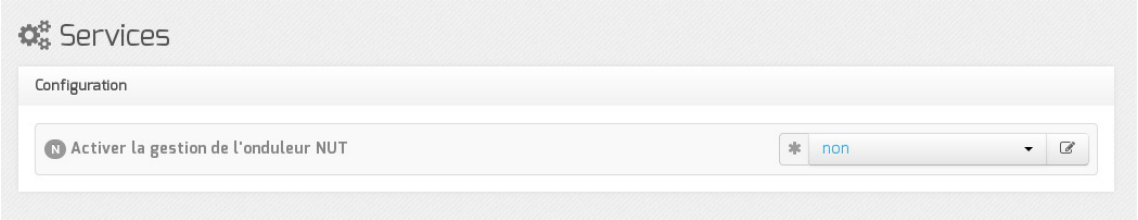
Voir aussi...

- Onglet Interface-n [p.27]

Les différentes mises à jour

Bases de filtres optionnels [p.223]

3.2. Onglet Services



Vue de l'onglet Services en mode normal

Le service de base commun à tous les modules est la gestion de l'onduleur NUT[p.309].

Les services de base propres au module Amon sont les suivants :

- l'anti-virus ClamAv ;
- le relai DHCP ;
- le réseau virtuel privé RVP ;
- le serveur EoleSSO ;
- le support WPAD ;
- le proxy inverse Nginx.

En mode expert les services de base communs à tous les modules sont :

- gestion des logs centralisés ;
- interface web de l'EAD.

En mode expert le seul service propre au module Amon est le filtrage sur le proxy qui est activé par défaut.

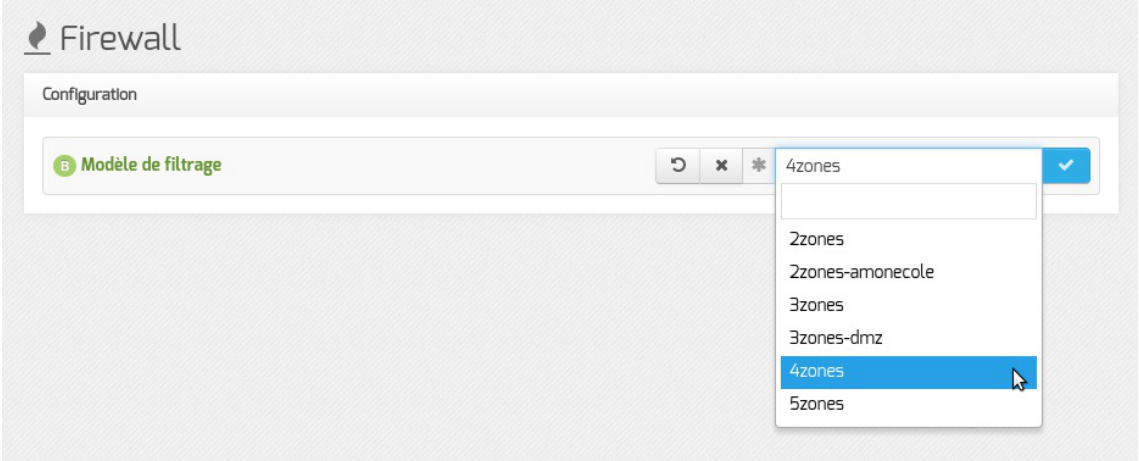
Voir aussi...

Onglet Logs : Gestion des logs centralisés

3.3. Onglet Firewall

Modèle de filtrage

Le modèle de filtrage doit être choisi en fonction du nombre d'interfaces activées et des services que l'on souhaite mettre en place.



Par convention le premier caractère des modèles de filtrage proposés est un chiffre qui correspond au nombre d'interfaces désirées.

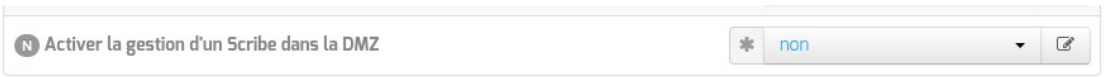
Les modèles de zone par défaut proposés supportent jusqu'à 5 cartes réseau :

- **2zones** : gestion d'une zone admin ou pedago sur eth1 ;
- **2zones-amonecole** : modèle spécifique au module AmonEcole (pedago sur eth1) ;
- **3zones** : gestion d'une zone admin sur eth1 et d'une zone pedago sur eth2 ;
- **3zones-dmz** : gestion d'une zone pedago sur eth1 et d'une zone DMZ publique pouvant accueillir un module Scribe sur eth2 ;
- **4zones** : gestion d'une zone admin sur eth1, d'une zone pedago sur eth2 et d'une zone DMZ publique pouvant accueillir un module Scribe sur eth3 ;
- **5zones** : gestion d'une zone admin sur eth1, d'une zone pedago sur eth2, d'une zone DMZ publique pouvant accueillir un module Scribe sur eth3 et d'une zone DMZ privée sur eth4.

Le modèle de zone proposés correspondent à un modèle de filtrage ERA. Les modèles de filtrage ERA sont la description de pare-feu enregistrés dans des fichiers XML situés par défaut dans le répertoire `/usr/share/era/modeles/`.

Avec ERA il est possible de créer un nouveau modèle personnalisé dans le répertoire `/usr/share/era/modeles/`. Celui-ci apparaîtra dans la liste des modèles proposés par défaut.

La variable `Activer la gestion d'un Scribe dans la DMZ` permet la prise en charge par bastion[p.302] des règles propres à la DMZ[p.304].



Si l'on souhaite mettre en place l'architecture suivante avec Amon :

- un réseau administratif ;
- un réseau pédagogique ;

- une DMZ contenant un serveur Scribe hébergeant des services web à ouvrir depuis l'extérieur.

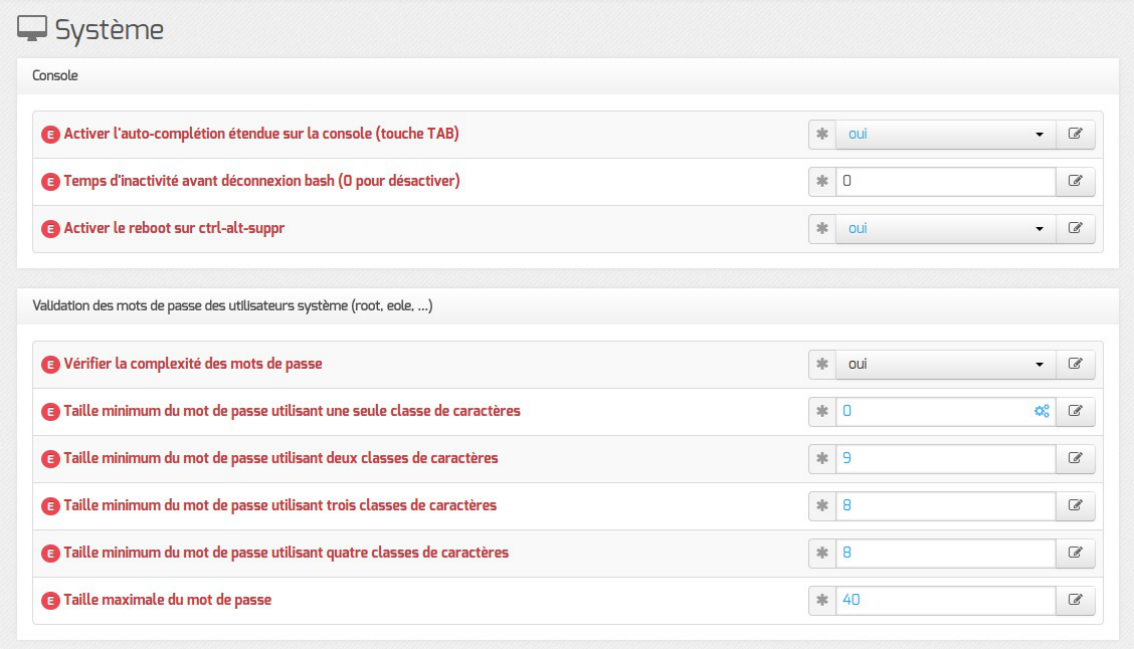
La configuration recommandée sera :

- `Nombre d'interfaces à activer` : `4` (onglet `Général` en mode basique) ;
- `Modèle de filtrage` : `4zones` (onglet `Firewall` en mode basique) ;
- `Activer la gestion d'un Scribe dans la DMZ` : `oui` (onglet `Firewall` en mode normal).

Voir aussi...

Configuration du module Amon avec le module Scribe en DMZ [p.187]

3.4. Onglet Système



Les paramètres de l'onglet `Système` permettent de régler le comportement de la console et de déterminer le niveau de complexité requis pour les mots de passe des utilisateurs système.

Paramétrage de la console

- `Activer l'auto-complétion étendue sur la console` : l'auto-complétion facilite l'utilisation de la ligne de commande mais peut ralentir son affichage, elle est activée par défaut ;
- `Temps d'inactivité avant déconnexion bash` : si aucune activité n'est constatée sur la console utilisateur pendant cette durée (en secondes), sa session est automatiquement coupée, avec le message : `attente de données expirée : déconnexion automatique`. La valeur `0` permet de désactiver cette fonctionnalité ;

- `Activer le reboot sur ctrl-alt-suppr` : si cette variable est passée à `non`, la séquence ctrl - alt - suppr est désactivée et affiche le message suivant `Control-Alt-Delete - séquence désactivée`.

Optimisations système

- `Poids relatif de l'utilisation de la swap par rapport à la mémoire vive` : Le swappiness est un paramètre du noyau Linux permettant de définir avec quelle sensibilité il va écrire dans la swap si la quantité de RAM à utiliser devient trop importante. Le système accepte des valeurs comprises entre 0 et 100. La valeur `0` empêchera au maximum le système d'utiliser la partition d'échange.
- `Activer le service de génération de nombres aléatoires rng-tools` : Le démon `rngd` agit comme une passerelle entre un vrai générateur de nombres aléatoires, matériel (TRNG), tel que ceux que l'on peut trouver dans les puces Intel/AMD/VIA et le pseudo-générateur de nombres aléatoires du noyau (PRNG).

Sur les serveurs virtualisés, le service `rngd` ne sera généralement pas fonctionnel et affichera, au démarrage, un message du type :

`erreur Starting Hardware RNG entropy gatherer daemon: (failed)`

Validation des mots de passe

EOLE propose un système de vérification des mots de passe évolué pour les utilisateurs système.

Un paramétrage a été mis par défaut, mais il est possible d'affiner les paramètres proposés.

La question `Vérifier la complexité des mots de passe` permet d'activer ou de désactiver la validation des mots de passe.

Si la vérification de la complexité des mots de passe est activée, celle-ci peut être régler plus finement à l'aide des paramètres suivants :

- `Taille minimum du mot de passe utilisant une seule classe de caractères` ;

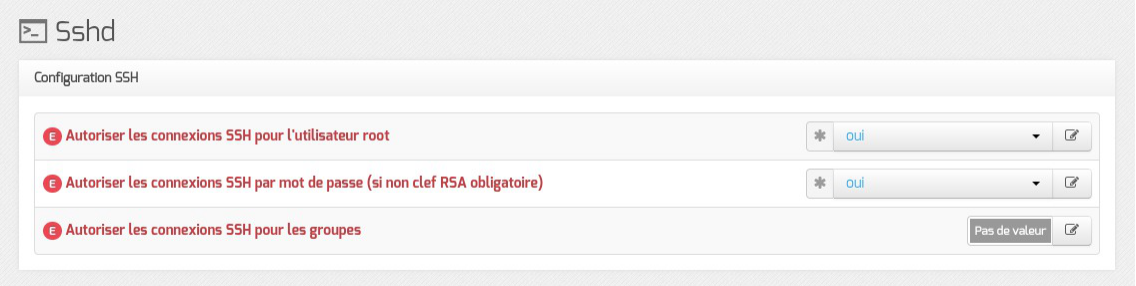
- `Taille minimum du mot de passe utilisant deux classes de caractères` ;
- `Taille minimum du mot de passe utilisant trois classes de caractères` ;
- `Taille minimum du mot de passe utilisant quatre classes de caractères` ;
- `Taille maximale du mot de passe`.

Plus d'informations sur le site du projet : http://www.openwall.com/passwdqc/

Les mots de passe (cf. Les mots de passe)

Ce paramétrage ne concerne que les comptes locaux. Les utilisateurs LDAP ne sont pas soumis aux mêmes restrictions.

3.5. Onglet Sshd : Gestion SSH avancée



Les paramètres disponibles dans cet onglet permettent d'affiner la configuration des accès SSH au serveur et viennent en complément des variables définissant les autorisations d'administration à distance saisies au niveau de chacune des interfaces (onglets `Interface-n`).

Ils permettent :

- d'interdire à l'utilisateur `root` de se connecter ;
- de n'autoriser que les connexions par clef RSA ;
- de déclarer des groupes Unix supplémentaires autorisés à se connecter en SSH au serveur.

Si les connexions par mots de passe sont interdites, une tentative de connexion sans clé valide entraînera l'affichage du message suivant :

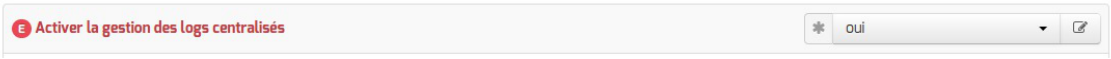
`Permission denied (publickey).`

Par défaut les groupes Unix autorisés sont `root` et `adm`.

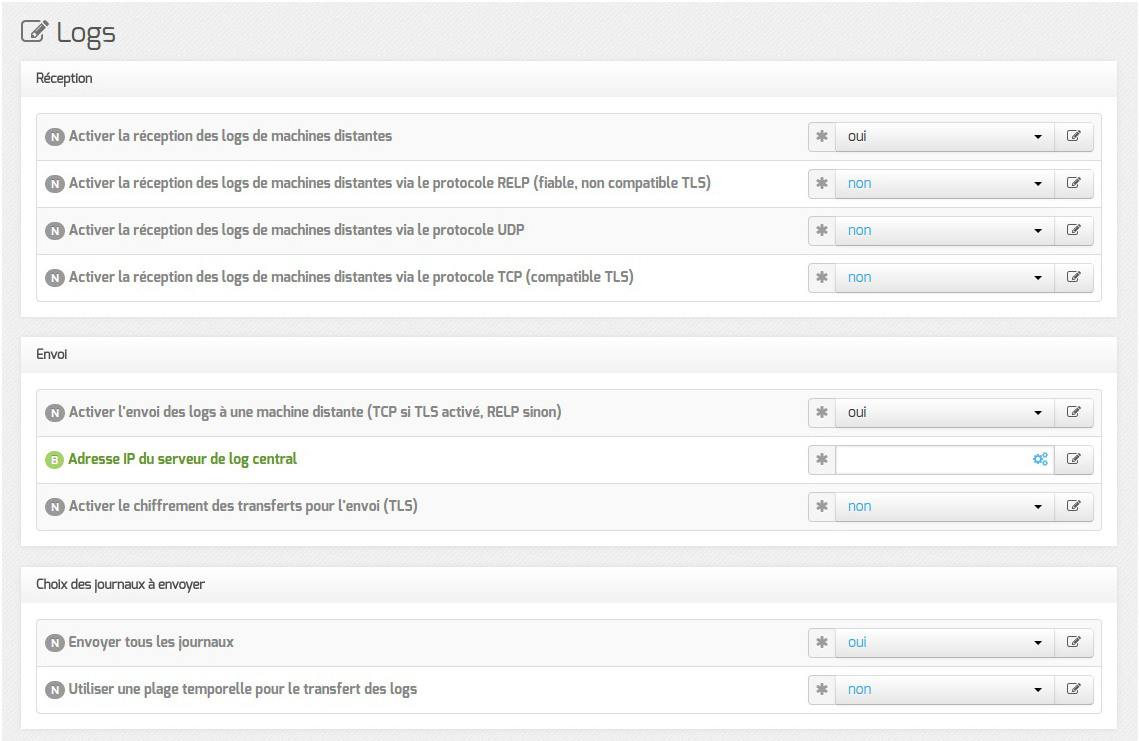
3.6. Onglet Logs : Gestion des logs centralisés

La possibilité de centraliser des logs a été dissociée de la mise en place d'un serveur ZéphirLog[p.315]. Cela rend possible un transfert croisé des journaux ou une centralisation.

Le support des logs centralisés peut être activé dans l'onglet `Service` en mode expert.



Cette activation affiche un nouvel onglet nommé `Logs` dans l'interface de configuration du module.



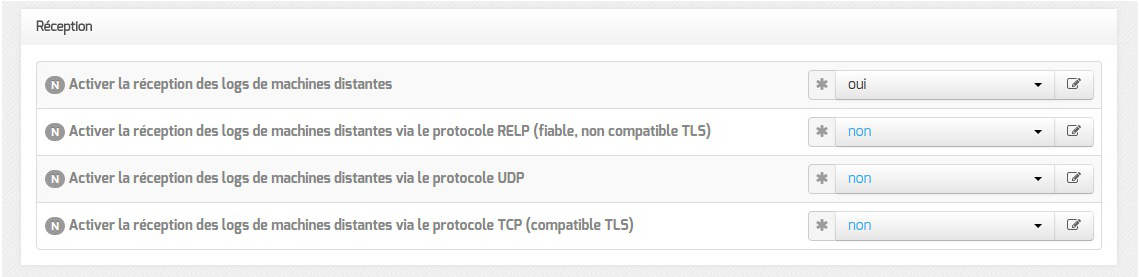
Vue de l'onglet Logs

Les options de cet onglet sont répartis en plusieurs sections :

- la configuration de la réception des logs permet de spécifier les protocoles de communication entre des machines distantes émettrices identifiées par leur adresse IP et le poste configuré ;
- la configuration de l'envoi des logs permet de spécifier l'adresse de la machine distante réceptrice. Le protocole (TCP ou RELP) utilisé est contraint par l'activation ou non du chiffrement (TLS) ;
- la configuration des journaux à envoyer permet de sélectionner les journaux à envoyer ainsi que l'heure de début et de fin de transfert.

Réception des journaux

Si la réception des journaux est activée (`Activer la réception des logs de machines distantes` à `oui`), il est possible de choisir jusqu'à 3 protocoles de réception : RELP, UDP et TLS over TCP.



L'activation des protocoles ouvre les ports adéquats sur le module.

Lorsque vous pouvez choisir les protocoles d'envoi et de réception des journaux, pensez à suivre les préconisations de l'ANSSI.

Envoi des journaux

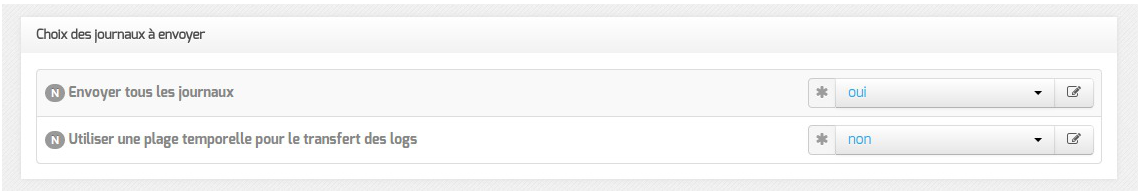
L'activation de l'envoi des journaux (`Activer l'envoi des logs à une machine distante` à `oui`) nécessite la saisie de l'adresse IP du serveur centralisateur de journaux.

Le protocole (TLS over TCP ou RELP) utilisé est contraint par l'activation ou non du chiffrement (TLS).

Lorsque vous pouvez choisir les protocoles d'envoi et de réception des journaux, pensez à suivre les préconisations de l'ANSSI.

Choix des journaux à envoyer

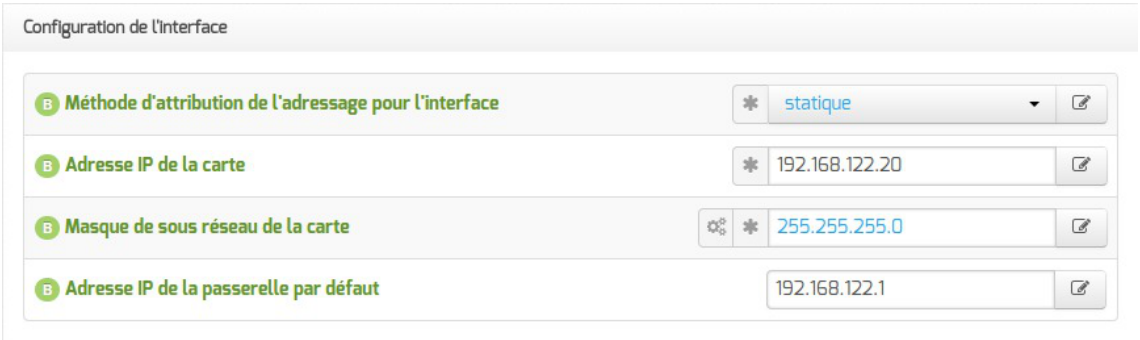
Si l'envoi des journaux est activé, il est possible d'envoyer tous les journaux ou de choisir les journaux à envoyer.



Il est également possible d'envoyer les journaux en temps réel ou en différé. L'heure de début et de fin (plage temporelle) de transfert des journaux est également paramétrable.

3.7. Onglet Interface-0

Configuration de l'interface



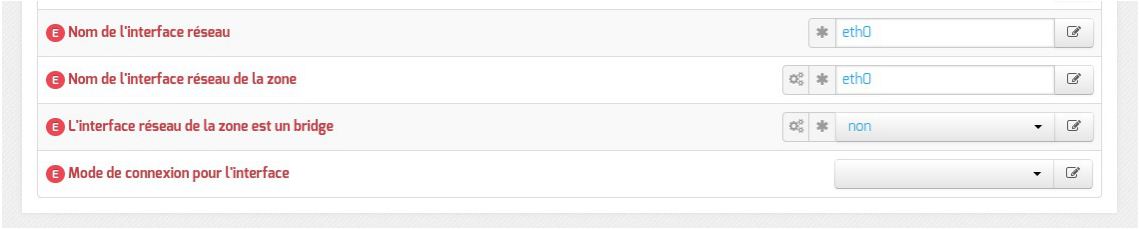
Configuration de l'interface

Avant toute chose, il faut savoir comment la carte réseau est configurée. Pour cela, il existe trois possibilités : statique, DHCP[p.303] et PPPoE[p.311].

- Dans le cas de la configuration statique, il faut renseigner l'adresse IP, le masque et la passerelle.
- La configuration DHCP ne nécessite aucun paramétrage particulier.
- En mode PPPoE, l'identifiant et le mot de passe de la connexion sont à renseigner.

EOLE est pleinement fonctionnel avec une connexion en IP fixe. Si vous ne disposez pas d'IP fixe, certaines fonctionnalités ne seront plus disponibles.

En mode expert quelques variables supplémentaires sont disponibles.



Nom de l'interface réseau

Le nom de l'interface est proposé dans l'interface de configuration du module est de la forme `eth0` mais celui-ci ne correspond pas toujours à la réalité du système. Il peut donc être adapté prendre la forme utilisé par le système, par exemple `em0`.

Le changement de nom d'une interface réseau dans le système se fait en éditant le fichier `/etc/udev/rules.d/70-persistent-net.rules`.

Un rechargement du module réseau ou plus simplement un redémarrage du système est nécessaire pour la prise en charge du changement.

Nom de l'interface réseau de la zone

Ce champ permet de personnaliser le nom de l'interface réseau de la zone.

L'interface réseau de la zone est un bridge

S'il existe un pont sur l'interface il est possible d'appliquer la configuration sur celui-ci en passant `L'interface réseau de la zone est un bridge` à `oui`. Il faut également saisir le nom du pont dans le champ `Nom de l'interface réseau de la zone`.

L'option ne crée pas le pont sur l'interface.

Mode de connexion pour l'interface

Le paramètre nommé `Mode de connexion pour l'interface` pour l'interface-0 et nommé `Mode de connexion pour l'interface interne-x` pour les autres interfaces permet de

forcer les propriétés de la carte réseau.

Par défaut, toutes les interfaces sont en mode `auto négociation`.

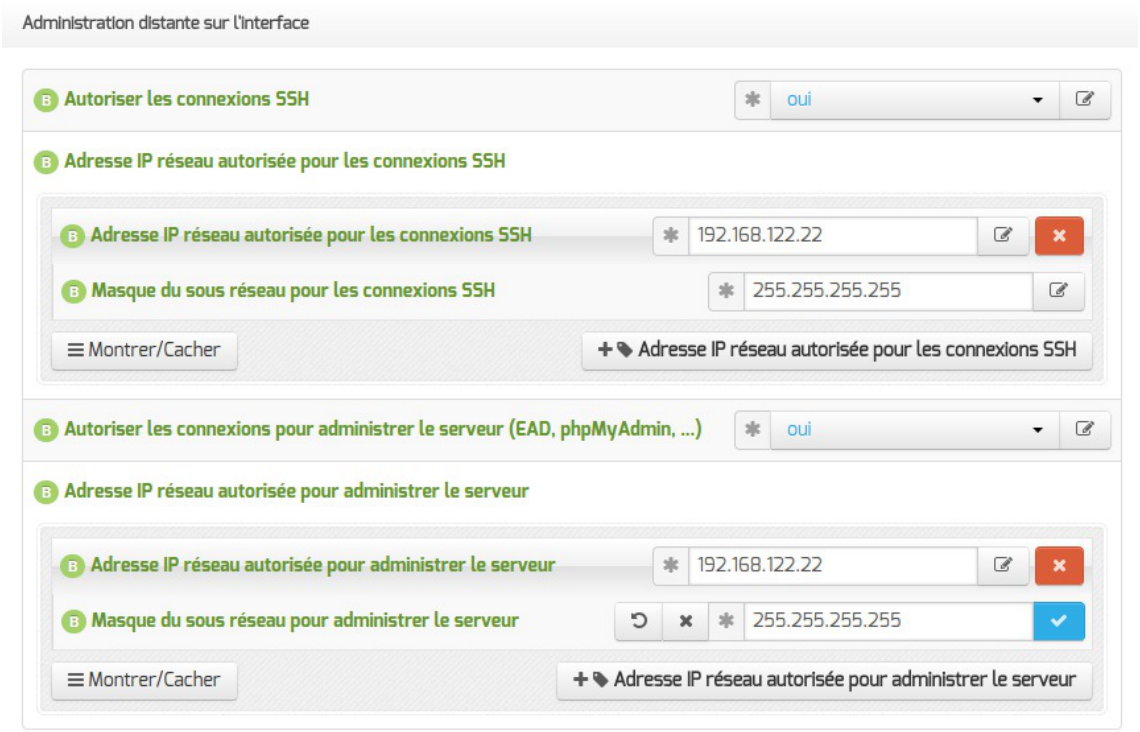
Ces paramètres ne devraient être modifiés que s'il y a un problème de négociation entre un élément actif et une des cartes réseau, tous les équipements modernes gérant normalement l'auto-négociation.

Liste des valeurs possible :

- `speed 100 duplex full autoneg off` : permet de forcer la vitesse à 100Mbits/s en full duplex sans chercher à négocier avec l'élément actif en face ;
- `autoneg on` : active l'auto-négociation (mode par défaut) :
- `speed 10 duplex half autoneg off` : permet de forcer la vitesse à 10Mbits/s en half duplex et désactiver l'auto-négociation ;
- `speed 1000 duplex full autoneg off` : permet de forcer la vitesse à 1Gbits/s en full duplex et désactiver l'auto-négociation.

Plus d'informations : http://fr.wikipedia.org/wiki/Auto-négociation_(ethernet).

Administration à distance

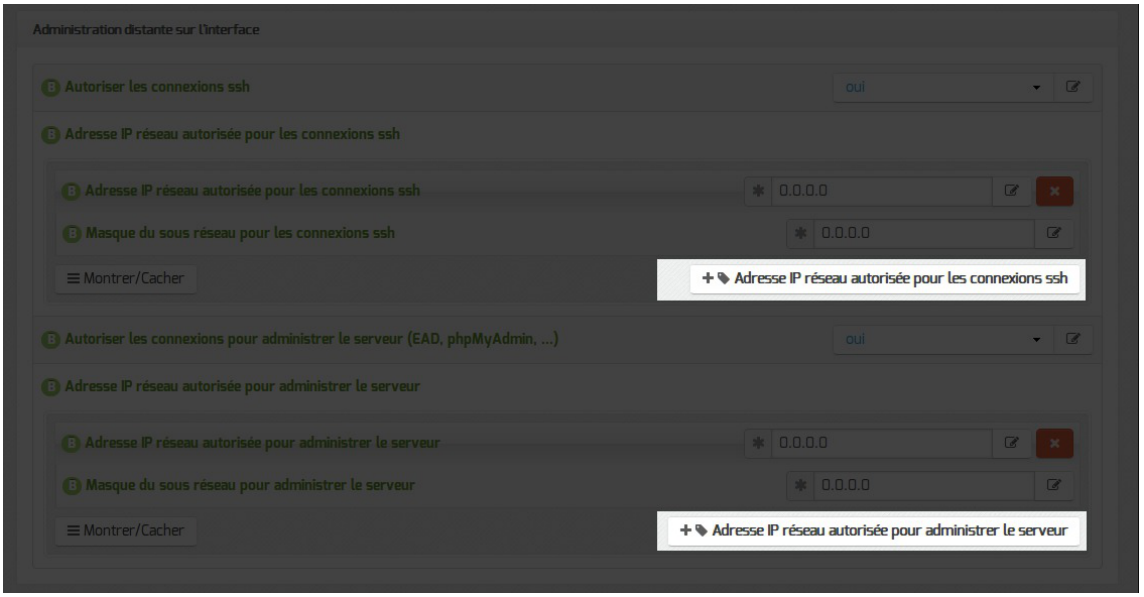


Configuration de l'administration à distance sur une interface

Par défaut les accès SSH[p.313] et aux différentes interfaces d'administration (EAD, phpMyAdmin, CUPS, ARV... selon le module) sont bloqués.

Pour chaque interface réseau activée (onglets `Interface-n`), il est possible d'autoriser des adresses IP ou des adresses réseau à se connecter.

Les adresses autorisées à se connecter via SSH sont indépendantes de celles configurées pour accéder aux interfaces d'administration.



Il est possible d'autoriser plusieurs adresses en cliquant sur `Adresse IP réseau autorisée pour…`.

Le masque réseau d'une station isolée est `255.255.255.255`.

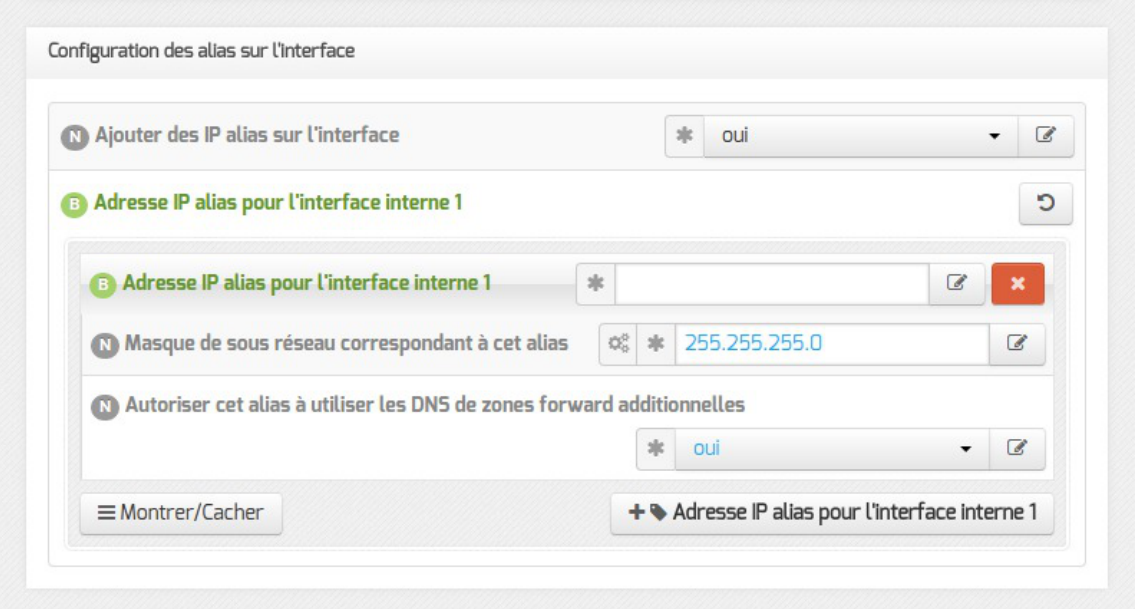
Dans le cadre de test sur un module l'utilisation de la valeur `0.0.0.0` dans les champs `Adresse IP réseau autorisée pour les connexions SSH` et `Masque du sous réseau pour les connexions SSH` autorise les connexions SSH depuis n'importe quelle adresse IP.

La commande suivante permet d'observer les connexions SSH arrivant sur un serveur EOLE : `tcpdump -nni $(CreoleGet nom_carte_eth0) port 22`

Des restrictions supplémentaires au niveau des connexions SSH sont disponibles dans l'onglet `Sshd` en mode expert.

Configuration des alias sur l'interface

EOLE supporte les alias sur les cartes réseau. Définir des alias IP consiste à affecter plus d'une adresse IP à une interface.



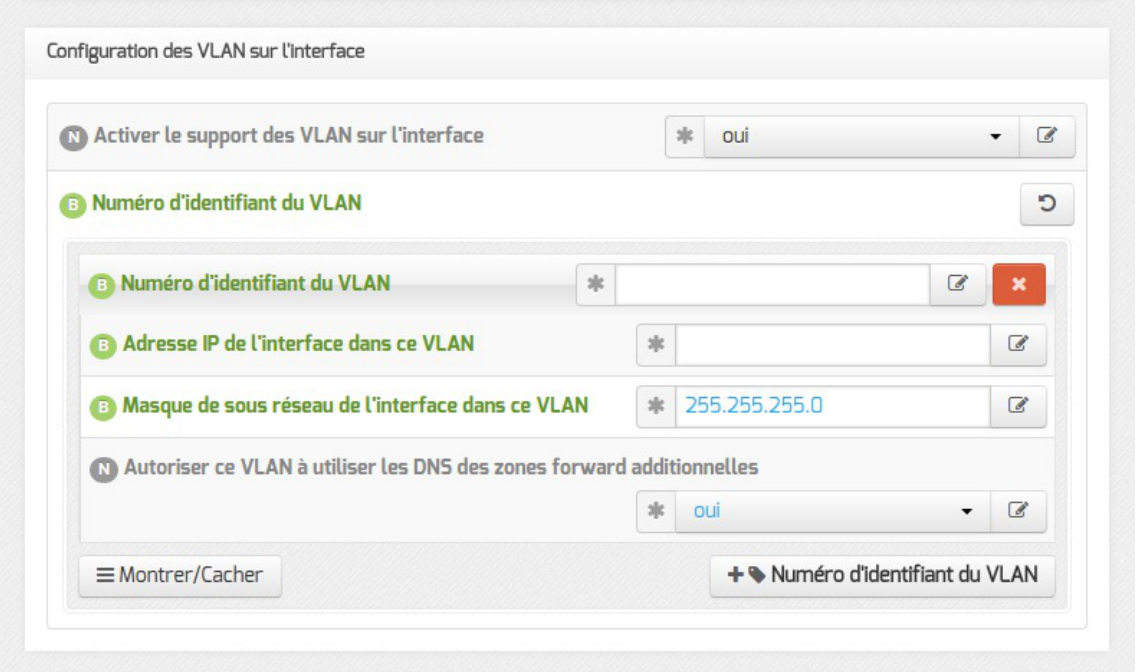
Pour cela, il faut activer son support (`Ajouter des IP alias sur l'interface` à `oui`) et configurer l'adresse IP et le masque de sous réseau.

Il est possible de configurer une passerelle particulière pour cet alias, ce paramètre est obligatoire si l'agrégation de liens est activée.

`Autoriser cet alias à utiliser les DNS de zones forward additionnelles` permet d'autoriser le réseau de cet alias à résoudre les noms d'hôte des domaines déclarés dans la section Forward de zone DNS de l'onglet `Zones-dns`.

Configuration des VLAN sur l'interface

Il est possible de configurer des VLAN (réseau local virtuel) sur une interface déterminée du module.



Pour cela, il faut activer son support (`Activer le support des VLAN sur l'interface` à `oui` et ajout d'un numéro identifiant du VLAN avec le bouton `+ Numéro d'identifiant du VLAN`) et configurer l'ensemble des paramètres utiles (l'ID, l'adresse IP, ...).

`Autoriser ce VLAN à utiliser les DNS des zones forward additionnelles` permet d'autoriser le réseau de ce VLAN à résoudre les noms d'hôte des domaines déclarés dans la section Forward de zone DNS de l'onglet `Zones-dns`.

Configuration DNS sur l'interface-0

Sur une installation en mode une carte (exemple : EoleBase + `eole-dns`), le DNS est activable ou désactivable dans l'onglet `Interface-0` avec la variable : `Activer le serveur DNS sur cette zone`.

Configuration du DNS sur eth0

Sur le module Amon et ses variantes (AmonEcole, AmonEcole+), cette question est également présente dans l'onglet `Interface-0`.

Pour chacune des interfaces configurées, il est possible de préciser si le DNS est maître de la zone en passant la variable `Serveur master DNS sur cette zone` à `oui`.

Au moins une des zones doit être configurée en maître de la zone.

Voir aussi...

> Onglet Agrégation : Mise en place d'une répartition de charge ou d'une haute disponibilité [p.52]

3.8. Onglet Interface-1

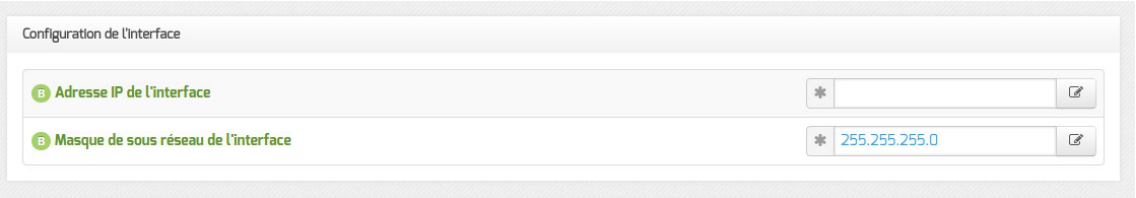
Nombre d'interfaces

Un module Amon peut avoir de 2 à 5 cartes réseau.

Le nombre d'interfaces activées se définit dans l'onglet `Général` de l'interface de configuration du module.

Cela ajoute autant d'onglets `Interface-n` que le nombre d'interfaces à activer choisi.

Configuration de l'interface



Configuration de l'interface

L'interface réseau nécessite un adressage statique, il faut renseigner l'adresse IP et le masque.

En mode expert quelques variables supplémentaires sont disponibles.

Nom de l'interface réseau

Le nom de l'interface est proposé dans l'interface de configuration du module est de la forme `eth0` mais celui-ci ne correspond pas toujours à la réalité du système. Il peut donc être adapté prendre la forme utilisé par le système, par exemple `em0`.

Le changement de nom d'une interface réseau dans le système se fait en éditant le fichier `/etc/udev/rules.d/70-persistent-net.rules`.

Un rechargement du module réseau ou plus simplement un redémarrage du système est nécessaire pour la prise en charge du changement.

Nom de l'interface réseau de la zone

Ce champ permet de personnaliser le nom de l'interface réseau de la zone.

L'interface réseau de la zone est un bridge

S'il existe un pont sur l'interface il est possible d'appliquer la configuration sur celui-ci en passant `L'interface réseau de la zone est un bridge` à `oui`. Il faut également saisir le nom du pont dans le champ `Nom de l'interface réseau de la zone`.

L'option ne crée pas le pont sur l'interface.

Mode de connexion pour l'interface

Le paramètre nommé `Mode de connexion pour l'interface` pour l'interface-0 et nommé `Mode de connexion pour l'interface interne-x` pour les autres interfaces permet de forcer les propriétés de la carte réseau.

Par défaut, toutes les interfaces sont en mode `auto négociation`.

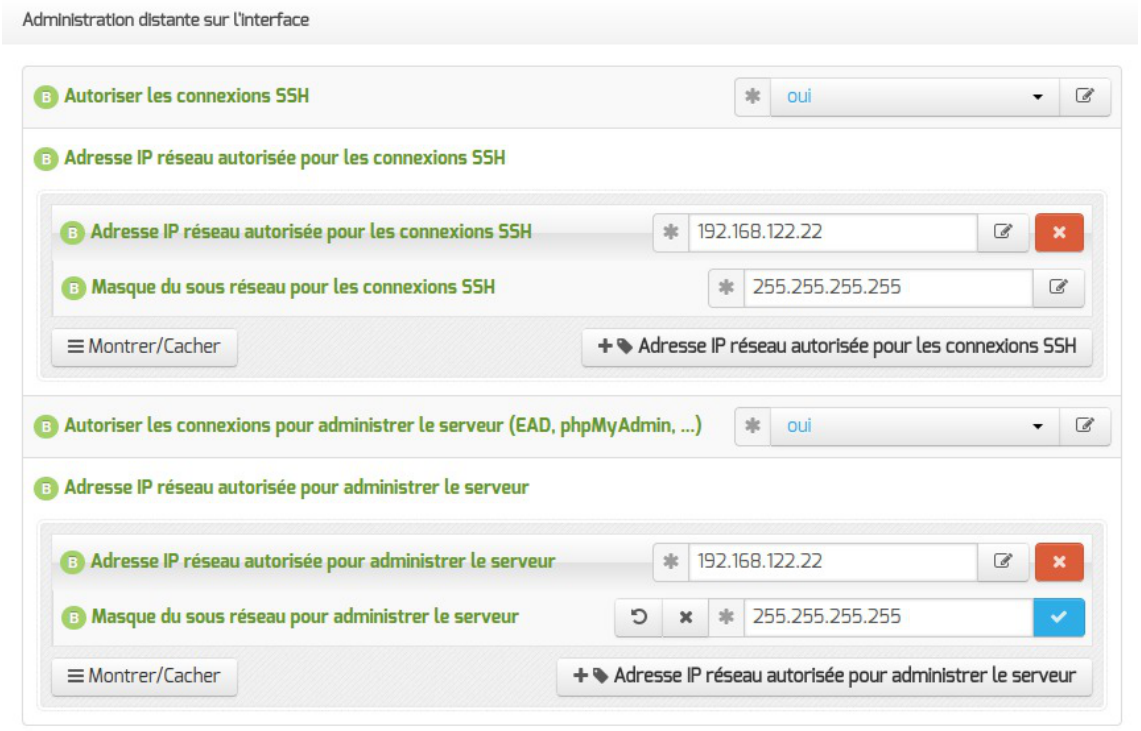
Ces paramètres ne devraient être modifiés que s'il y a un problème de négociation entre un élément actif et une des cartes réseau, tous les équipements modernes gérant normalement l'auto-négociation.

Liste des valeurs possible :

- `speed 100 duplex full autoneg off` : permet de forcer la vitesse à 100Mbits/s en full duplex sans chercher à négocier avec l'élément actif en face ;
- `autoneg on` : active l'auto-négociation (mode par défaut) :
- `speed 10 duplex half autoneg off` : permet de forcer la vitesse à 10Mbits/s en half duplex et désactiver l'auto-négociation ;
- `speed 1000 duplex full autoneg off` : permet de forcer la vitesse à 1Gbits/s en full duplex et désactiver l'auto-négociation.

Plus d'informations : http://fr.wikipedia.org/wiki/Auto-négociation_(ethernet).

Administration à distance

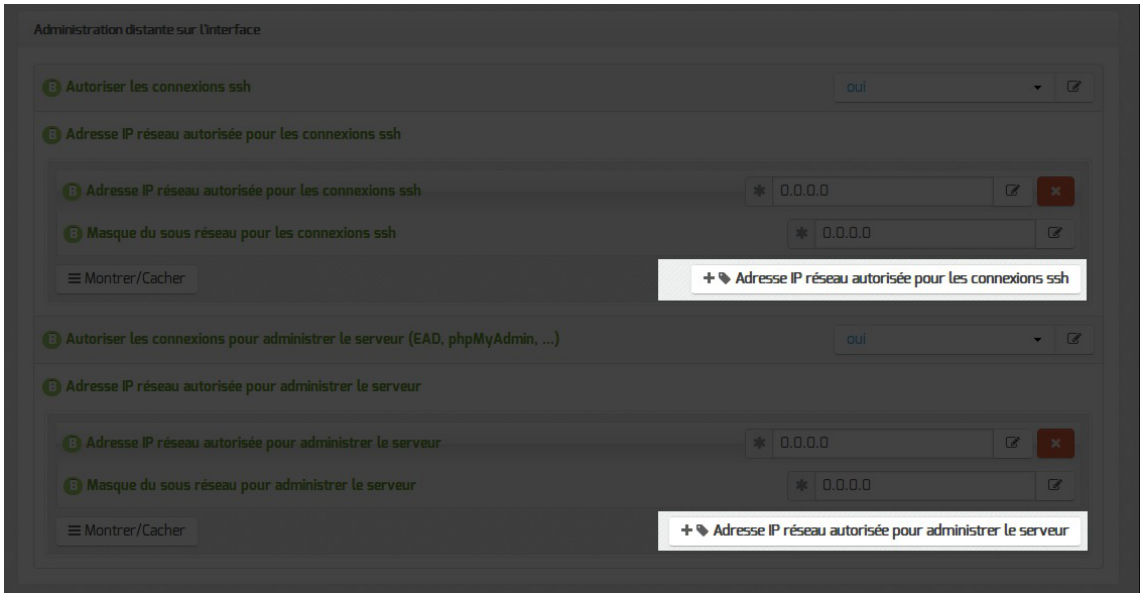


Configuration de l'administration à distance sur une interface

Par défaut les accès SSH[p.313] et aux différentes interfaces d'administration (EAD, phpMyAdmin, CUPS, ARV... selon le module) sont bloqués.

Pour chaque interface réseau activée (onglets `Interface-n`), il est possible d'autoriser des adresses IP ou des adresses réseau à se connecter.

Les adresses autorisées à se connecter via SSH sont indépendantes de celles configurées pour accéder aux interfaces d'administration.



Il est possible d'autoriser plusieurs adresses en cliquant sur `Adresse IP réseau autorisée pour…`.

Le masque réseau d'une station isolée est `255.255.255.255`.

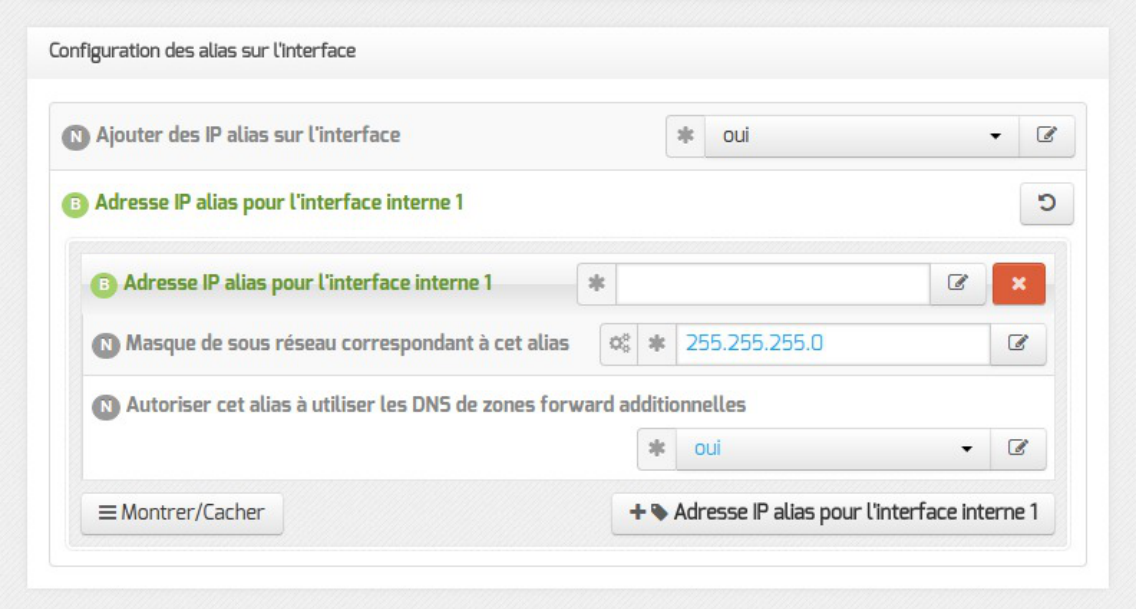
Dans le cadre de test sur un module l'utilisation de la valeur `0.0.0.0` dans les champs `Adresse IP réseau autorisée pour les connexions SSH` et `Masque du sous réseau pour les connexions SSH` autorise les connexions SSH depuis n'importe quelle adresse IP.

La commande suivante permet d'observer les connexions SSH arrivant sur un serveur EOLE : `tcpdump -nni $(CreoleGet nom_carte_eth0) port 22`

Des restrictions supplémentaires au niveau des connexions SSH sont disponibles dans l'onglet `Sshd` en mode expert.

Configuration des alias sur l'interface

EOLE supporte les alias sur les cartes réseau. Définir des alias IP consiste à affecter plus d'une adresse IP à une interface.

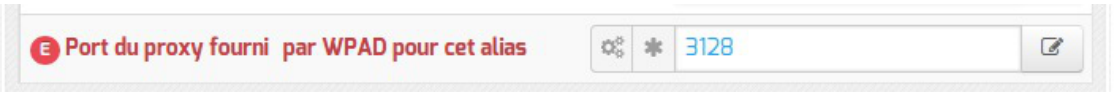


Pour cela, il faut activer son support (`Ajouter des IP alias sur l'interface` à `oui`) et configurer l'adresse IP et le masque de sous réseau.

Il est possible de configurer une passerelle particulière pour cet alias, ce paramètre est obligatoire si l'agrégation de liens est activée.

`Autoriser cet alias à utiliser les DNS de zones forward additionnelles` permet d'autoriser le réseau de cet alias à résoudre les noms d'hôte des domaines déclarés dans la section Forward de zone DNS de l'onglet `Zones-dns`.

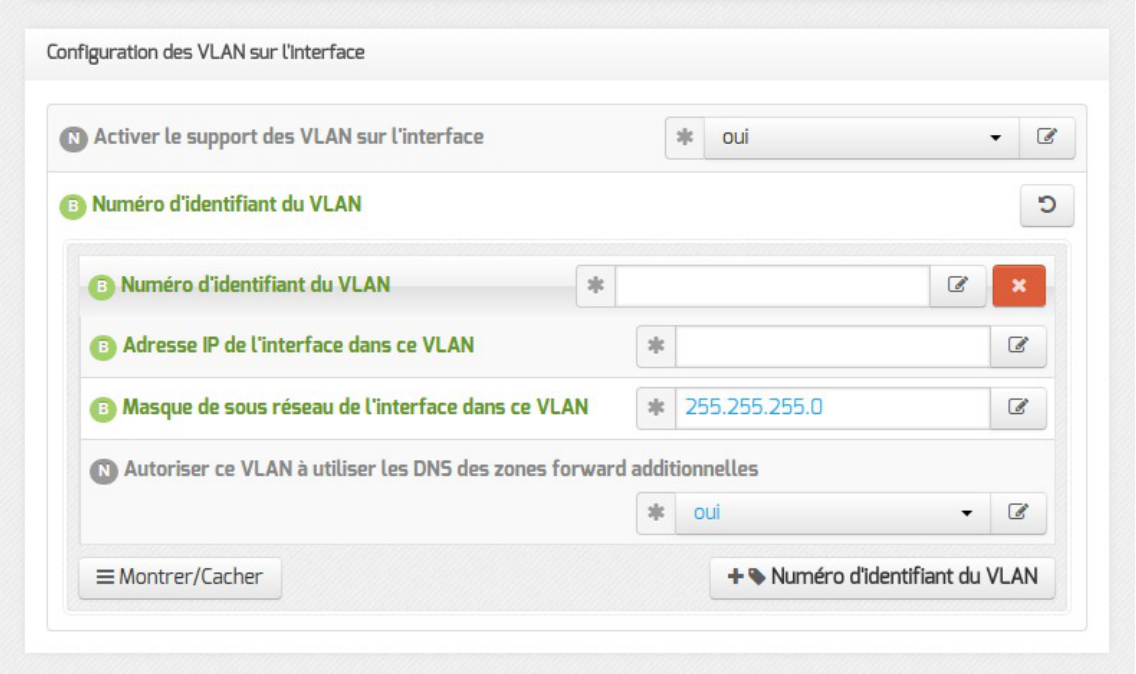
En mode expert si WPAD est activé il est possible de changer le port du proxy, 3128 par défaut, pour un alias donné.



Si l'authentification NTLM est activée, le port par défaut du proxy est 3127.

Configuration des VLAN sur l'interface

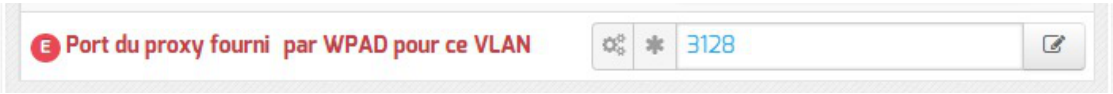
Il est possible de configurer des VLAN (réseau local virtuel) sur une interface déterminée du module.



Pour cela, il faut activer son support (`Activer le support des VLAN sur l'interface` à `oui` et ajout d'un numéro identifiant du VLAN avec le bouton `+ Numéro d'identifiant du VLAN`) et configurer l'ensemble des paramètres utiles (l'ID, l'adresse IP, ...).

`Autoriser ce VLAN à utiliser les DNS des zones forward additionnelles` permet d'autoriser le réseau de ce VLAN à résoudre les noms d'hôte des domaines déclarés dans la section Forward de zone DNS de l'onglet `Zones-dns`.

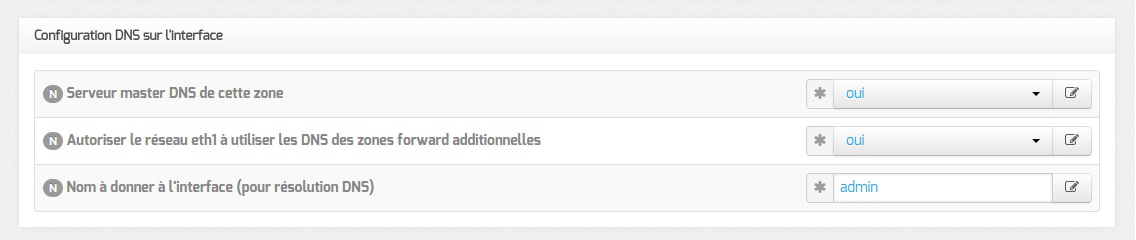
En mode expert si WPAD est activé il est possible de changer le port du proxy, 3128 par défaut, pour un VLAN donné.



Si l'authentification NTLM est activée, le port par défaut du proxy est 3127.

Configuration DNS sur l'interface

Il est possible d'ajuster les paramètres du serveur DNS pour chaque interface réseau sauf pour l'interface 0.



- `Serveur master DNS de cette zone` : sert à activer le DNS sur l'interface.
- `Autoriser le réseau ethX à utiliser les DNS des zones forward additionnels` : permet d'autoriser le réseau ethX à résoudre les noms d'hôte des domaines déclarés dans la section `Forward de zone DNS` de l'onglet `Zones-dns`.

- `Nom à donner à l'interface (pour résolution DNS)` : entrée DNS correspondant à l'adresse IP de l'interface ethX. Le nom par défaut (admin pour l'interface eth1) est différent et doit rester pour chaque interface.

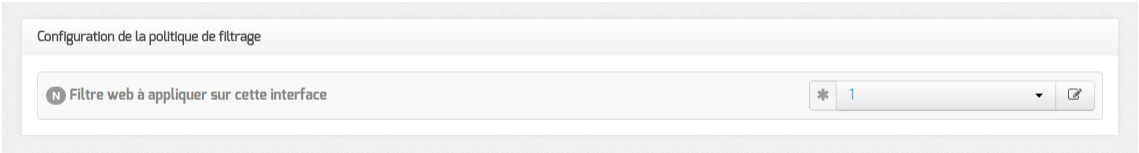
Si le support du RVP est activé une option supplémentaire est disponible :

- `Autoriser le réseau ethX à utiliser les DNS de forward RVP/AGRIATES` : Si le service RVP est activé (onglet `Services`) et que le serveur est membre du réseau AGRIATES (onglet `Rvp`) la variable est disponible pour autoriser ou non le réseau ethX à résoudre les noms d'hôte de la zone AGRIATES.

Configuration de la politique de filtrage

EOLE permet de différencier les zones suivant l'interface (administration ou pédagogie).

La différenciation se fait en modifiant la valeur choisie pour `Filtre Web à appliquer à cette interface` dans la configuration de chaque interface (onglets : `Interface-1`, `Interface-2`, ...).



Les filtres web 1 et 2 correspondent chacun à une instance du logiciel de filtrage. La configuration de chacun des filtres se fait dans l'onglet `Filtrage web`.

Voir aussi...

Onglet Filtrage web : Configuration du filtrage web [p.157]

3.9. Onglet Interface-n

Nombre d'interfaces

Un module Amon peut avoir de 2 à 5 cartes réseau.

Le nombre d'interfaces activées se définit dans l'onglet `Général` de l'interface de configuration du module.

Cela ajoute autant d'onglets `Interface-n` que le nombre d'interfaces à activer choisi.

Configuration de l'interface

Configuration de l'interface

L'interface réseau nécessite un adressage statique, il faut renseigner l'adresse IP et le masque.

En mode expert quelques variables supplémentaires sont disponibles.

Nom de l'interface réseau

Le nom de l'interface est proposé dans l'interface de configuration du module est de la forme `eth0` mais celui-ci ne correspond pas toujours à la réalité du système. Il peut donc être adapté prendre la forme utilisé par le système, par exemple `em0`.

Le changement de nom d'une interface réseau dans le système se fait en éditant le fichier `/etc/udev/rules.d/70-persistent-net.rules`.

Un rechargement du module réseau ou plus simplement un redémarrage du système est nécessaire pour la prise en charge du changement.

Nom de l'interface réseau de la zone

Ce champ permet de personnaliser le nom de l'interface réseau de la zone.

L'interface réseau de la zone est un bridge

S'il existe un pont sur l'interface il est possible d'appliquer la configuration sur celui-ci en passant `L'interface réseau de la zone est un bridge` à `oui`. Il faut également saisir le nom du pont dans le champ `Nom de l'interface réseau de la zone`.

L'option ne crée pas le pont sur l'interface.

Mode de connexion pour l'interface

Le paramètre nommé `Mode de connexion pour l'interface` pour l'interface-0 et nommé `Mode de connexion pour l'interface interne-x` pour les autres interfaces permet de forcer les propriétés de la carte réseau.

Par défaut, toutes les interfaces sont en mode `auto négociation`.

Ces paramètres ne devraient être modifiés que s'il y a un problème de négociation entre un élément actif et une des cartes réseau, tous les équipements modernes gérant normalement l'auto-négociation.

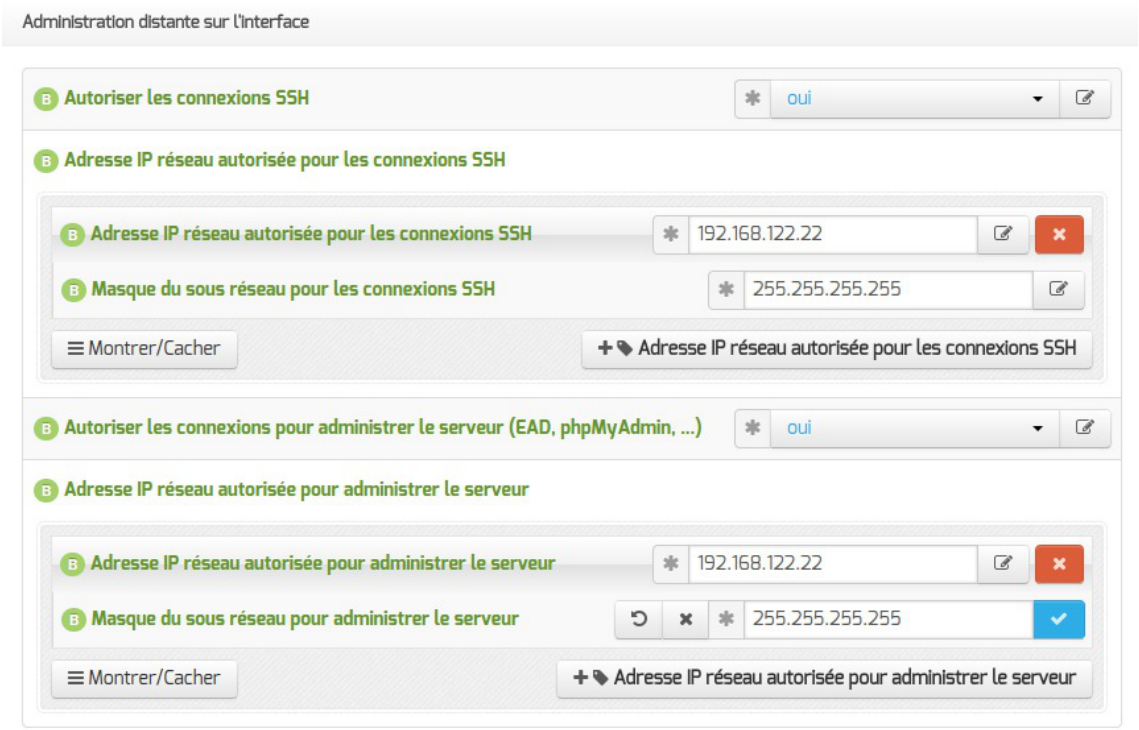
Liste des valeurs possible :

- `speed 100 duplex full autoneg off` : permet de forcer la vitesse à 100Mbits/s en full duplex sans chercher à négocier avec l'élément actif en face ;
- `autoneg on` : active l'auto-négociation (mode par défaut) :

- `speed 10 duplex half autoneg off` : permet de forcer la vitesse à 10Mbits/s en half duplex et désactiver l'auto-négociation ;
- `speed 1000 duplex full autoneg off` : permet de forcer la vitesse à 1Gbits/s en full duplex et désactiver l'auto-négociation.

Plus d'informations : http://fr.wikipedia.org/wiki/Auto-négociation_(ethernet).

Administration à distance

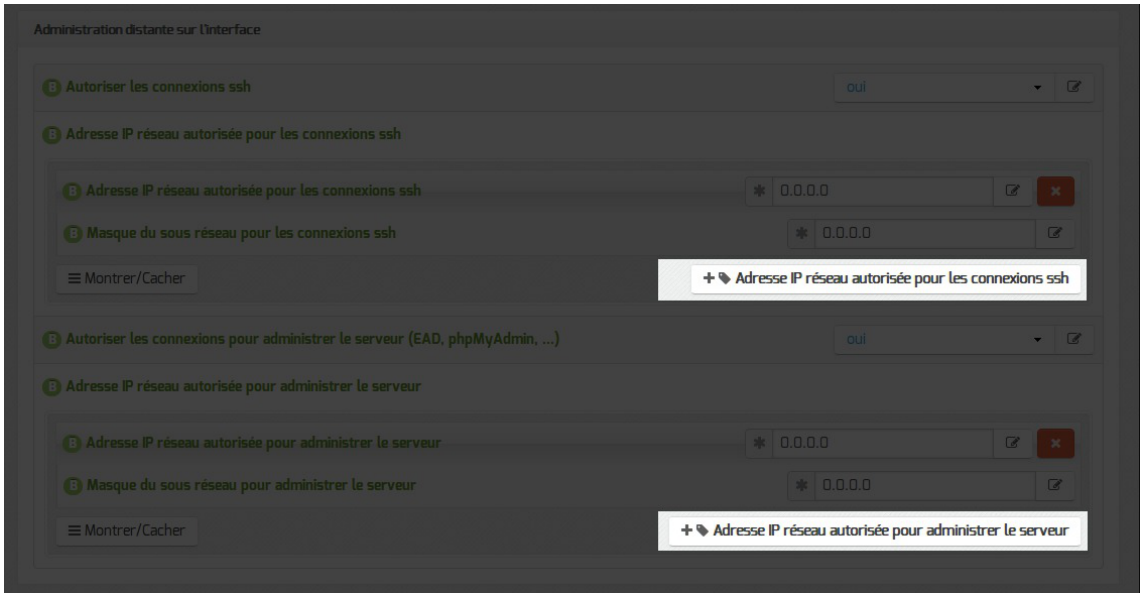


Configuration de l'administration à distance sur une interface

Par défaut les accès SSH[p.313] et aux différentes interfaces d'administration (EAD, phpMyAdmin, CUPS, ARV... selon le module) sont bloqués.

Pour chaque interface réseau activée (onglets `Interface-n`), il est possible d'autoriser des adresses IP ou des adresses réseau à se connecter.

Les adresses autorisées à se connecter via SSH sont indépendantes de celles configurées pour accéder aux interfaces d'administration.



Il est possible d'autoriser plusieurs adresses en cliquant sur `Adresse IP réseau autorisée pour…`.

Le masque réseau d'une station isolée est `255.255.255.255`.

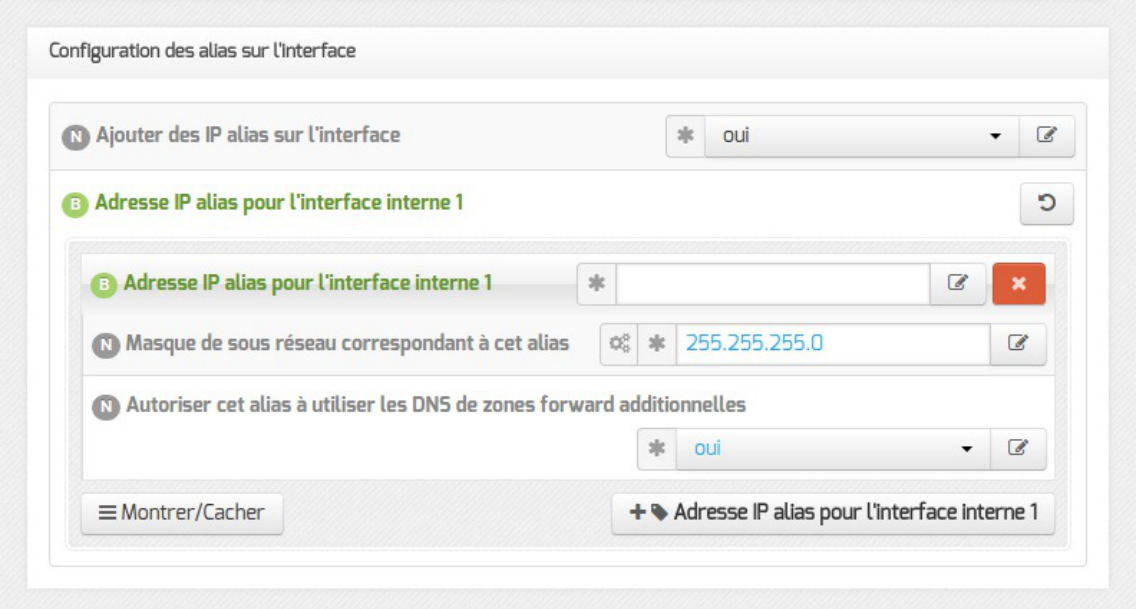
Dans le cadre de test sur un module l'utilisation de la valeur `0.0.0.0` dans les champs `Adresse IP réseau autorisée pour les connexions SSH` et `Masque du sous réseau pour les connexions SSH` autorise les connexions SSH depuis n'importe quelle adresse IP.

La commande suivante permet d'observer les connexions SSH arrivant sur un serveur EOLE : `tcpdump -nni $(CreoleGet nom_carte_eth0) port 22`

Des restrictions supplémentaires au niveau des connexions SSH sont disponibles dans l'onglet `Sshd` en mode expert.

Configuration des alias sur l'interface

EOLE supporte les alias sur les cartes réseau. Définir des alias IP consiste à affecter plus d'une adresse IP à une interface.

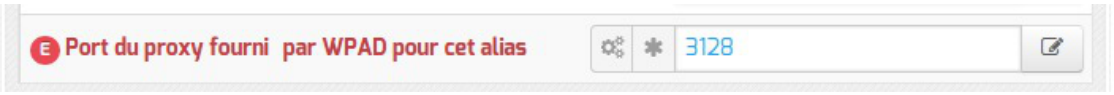


Pour cela, il faut activer son support (`Ajouter des IP alias sur l'interface` à `oui`) et configurer l'adresse IP et le masque de sous réseau.

Il est possible de configurer une passerelle particulière pour cet alias, ce paramètre est obligatoire si l'agrégation de liens est activée.

`Autoriser cet alias à utiliser les DNS de zones forward additionnelles` permet d'autoriser le réseau de cet alias à résoudre les noms d'hôte des domaines déclarés dans la section Forward de zone DNS de l'onglet `Zones-dns`.

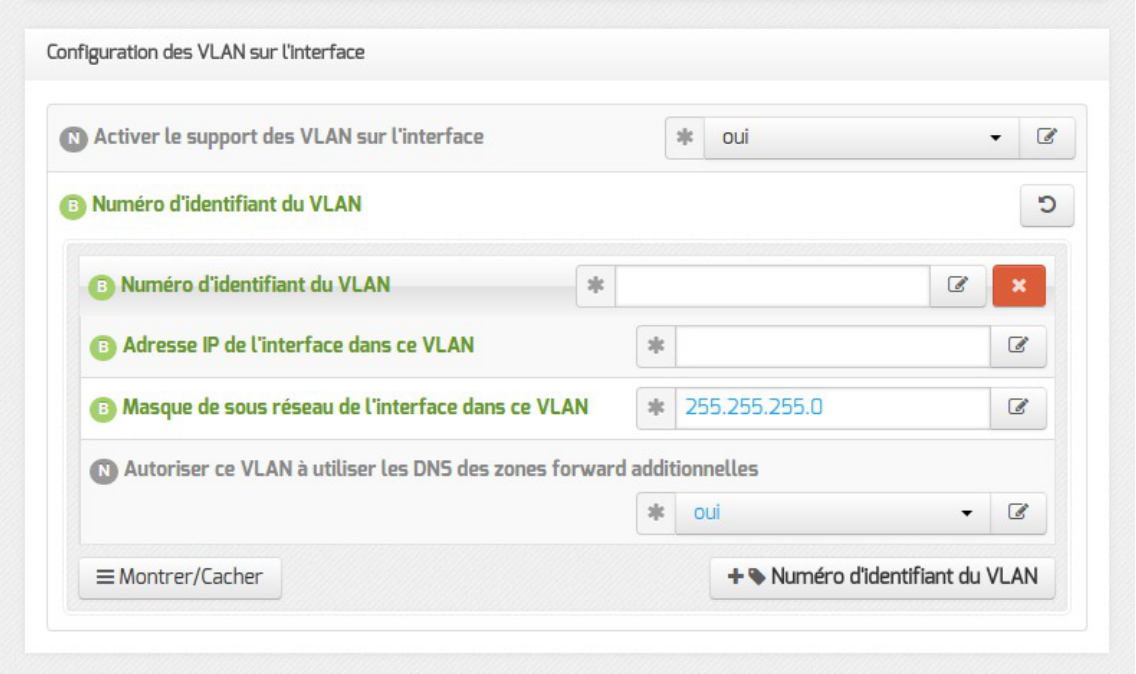
En mode expert si WPAD est activé il est possible de changer le port du proxy, 3128 par défaut, pour un alias donné.



Si l'authentification NTLM est activée, le port par défaut du proxy est 3127.

Configuration des VLAN sur l'interface

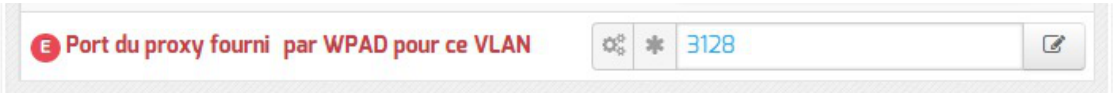
Il est possible de configurer des VLAN (réseau local virtuel) sur une interface déterminée du module.



Pour cela, il faut activer son support (`Activer le support des VLAN sur l'interface` à `oui` et ajout d'un numéro identifiant du VLAN avec le bouton `+ Numéro d'identifiant du VLAN`) et configurer l'ensemble des paramètres utiles (l'ID, l'adresse IP, ...).

`Autoriser ce VLAN à utiliser les DNS des zones forward additionnelles` permet d'autoriser le réseau de ce VLAN à résoudre les noms d'hôte des domaines déclarés dans la section Forward de zone DNS de l'onglet `Zones-dns`.

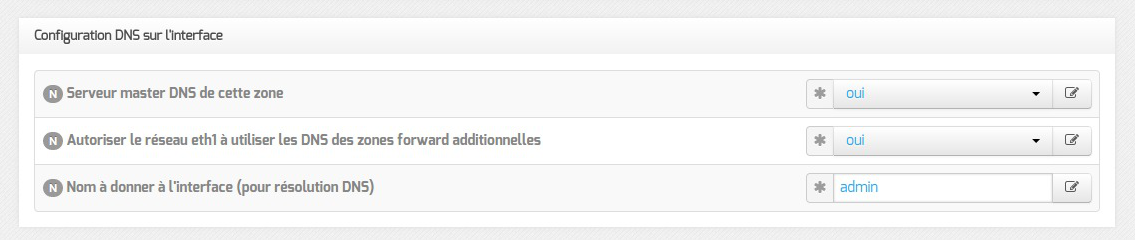
En mode expert si WPAD est activé il est possible de changer le port du proxy, 3128 par défaut, pour un VLAN donné.



Si l'authentification NTLM est activée, le port par défaut du proxy est 3127.

Configuration DNS sur l'interface

Il est possible d'ajuster les paramètres du serveur DNS pour chaque interface réseau sauf pour l'interface 0.



- `Serveur master DNS de cette zone` : sert à activer le DNS sur l'interface.
- `Autoriser le réseau ethX à utiliser les DNS des zones forward additionnels` : permet d'autoriser le réseau ethX à résoudre les noms d'hôte des domaines déclarés dans la section `Forward de zone DNS` de l'onglet `Zones-dns`.

- `Nom à donner à l'interface (pour résolution DNS)` : entrée DNS correspondant à l'adresse IP de l'interface ethX. Le nom par défaut (admin pour l'interface eth1) est différent et doit rester pour chaque interface.

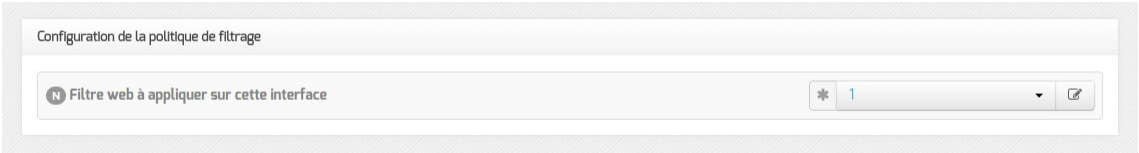
Si le support du RVP est activé une option supplémentaire est disponible :

- `Autoriser le réseau ethX à utiliser les DNS de forward RVP/AGRIATES` : Si le service RVP est activé (onglet `Services`) et que le serveur est membre du réseau AGRIATES (onglet `Rvp`) la variable est disponible pour autoriser ou non le réseau ethX à résoudre les noms d'hôte de la zone AGRIATES.

Configuration de la politique de filtrage

EOLE permet de différencier les zones suivant l'interface (administration ou pédagogie).

La différenciation se fait en modifiant la valeur choisie pour `Filtre Web à appliquer à cette interface` dans la configuration de chaque interface (onglets : `Interface-1`, `Interface-2`, ...).



Les filtres web 1 et 2 correspondent chacun à une instance du logiciel de filtrage. La configuration de chacun des filtres se fait dans l'onglet `Filtrage web`.

Voir aussi...

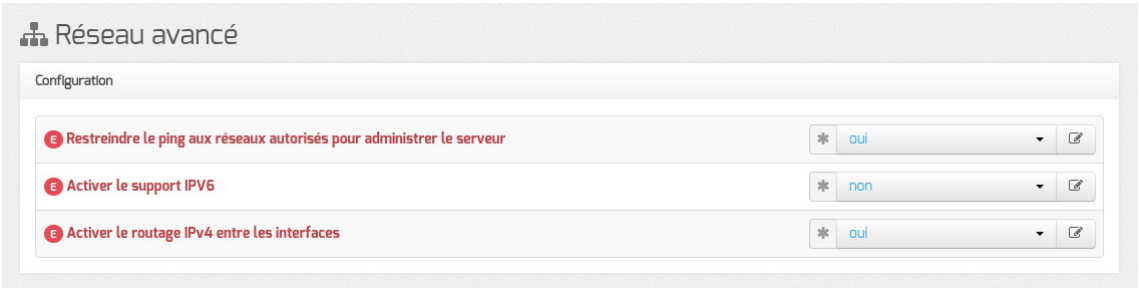
Onglet Filtrage web : Configuration du filtrage web [p.157]

Onglet Proxy authentifié : 5 méthodes d'authentification [p.74]

3.10. Onglet Réseau avancé

Présentation des différents paramètres de l'onglet `Réseau avancé` accessible en mode expert.

Configuration IP



Même si la fonctionnalité `Restreindre le ping aux réseaux autorisés pour administrer le serveur` apparaît dans l'onglet `Réseau avancé` du présent module, elle n'a aucun effet.

> C'est dans les modèles ERA que sont décrites les restrictions liées au protocole ICMP[p.306].

> À partir de la version 2.5.2, cette variable n'apparaît plus sur le présent module.

La variable `Activer le support IPv6` est par défaut à `non` et est utilisée pour désactiver explicitement le support de l'IPv6 dans la configuration de certains logiciels (BIND, Proftpd).

Le support de l'IPv6[p.307] peut être activé en passant la variable `Activer le support IPv6` à `oui` mais sa prise en charge ne se sera faite qu'au niveau du noyau.

Si la variable `Activer le routage IPv4 entre les interfaces` est à `oui`, alors le routage IPv4 est activé au niveau du noyau (`/proc/sys/net/ipv4/ip_forward` passe à `1`)

L'activation du support IPv6 entraîne l'apparition de la variable : `Activer le routage IPv6 entre les interfaces`.

Si cette dernière est à `oui` le routage IPv6 est activé au niveau du noyau (`/proc/sys/net/ipv6/conf/all/forwarding` passe à `1`).

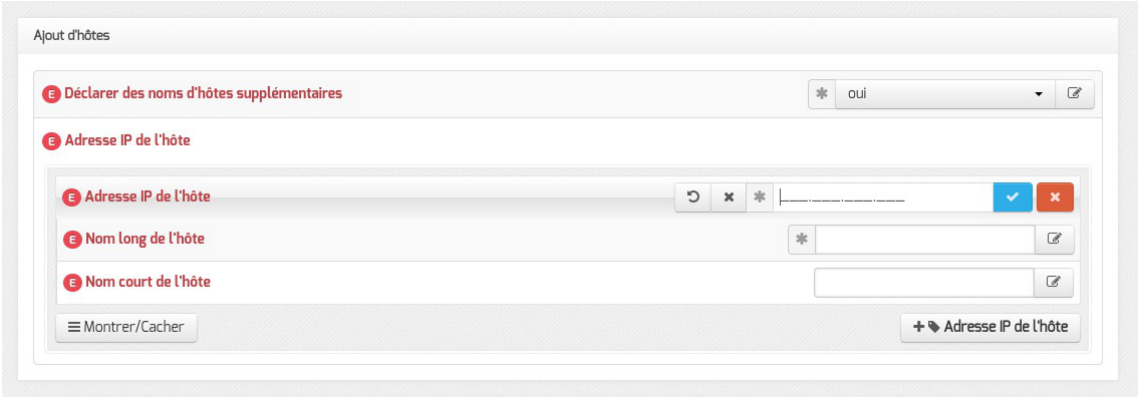
Sécurité

Si la variable `Journaliser les "martian sources"` est à `oui`, tous les passages de paquets utilisant des adresses IP réservées à un usage particulier (http://tools.ietf.org/html/rfc5735) seront enregistrées dans les journaux.

Par défaut, l'anti-spoofing[p.301] est activé sur l'interface-0 des modules EOLE.

Sur les serveurs ayant 2 interfaces réseau ou plus d'activées (cas par défaut pour Amon et Sphynx), il est possible de demander l'activation de l'anti-spoofing sur les autres interfaces en passant la variable `Activer l'anti-spoofing sur toutes les interfaces` à `oui`.

Ajout d'hôtes



En passant la variable `Déclarer des noms d'hôtes supplémentaires` à `oui` il est possible de déclarer des noms d'hôtes qui seront ajoutés au fichier `/etc/hosts`.

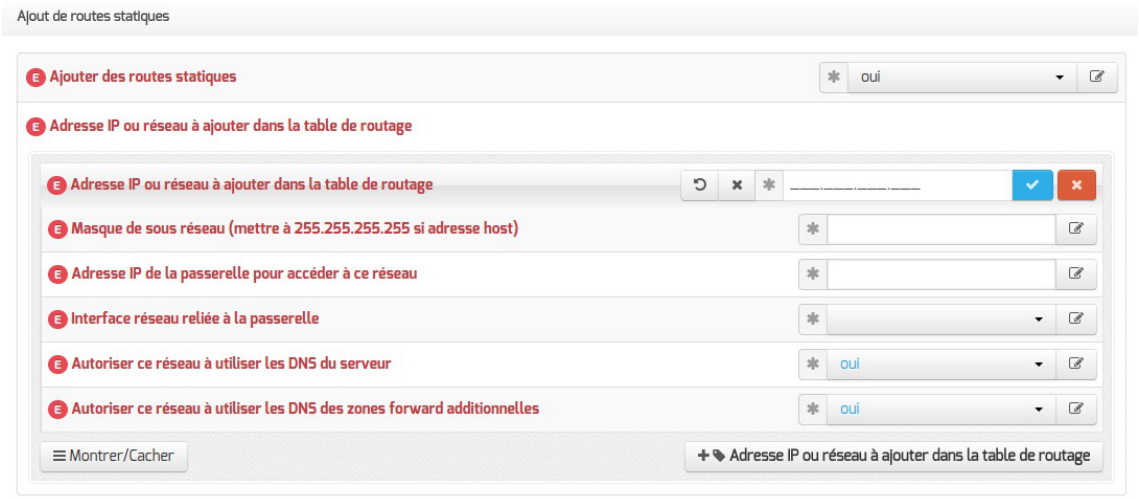
Il est possible d'ajouter plusieurs hôtes supplémentaires en cliquant sur le bouton `+Adresse IP de l'hôte` .

Sur un module avec serveur DNS (module Amon), pour que le DNS puisse résoudre le nom, il faut que le suffixe DNS du nom long corresponde au `Nom de domaine privé du réseau local` saisi dans l'onglet `Général`.

Si ce n'est pas le cas, il faudra déclarer un nom de domaine local supplémentaire dans l'onglet `Réseau avancé` pour permettre au serveur DNS de résoudre ce nom d'hôte.

Le champ `Nom court de l'hôte` est optionnel.

Ajout de routes statiques



Ce bloc de paramètres permet d'ajouter, manuellement, des routes afin d'accéder à des adresses ou à des plages d'adresses par un chemin différent de celui par défaut (défini par le routeur par défaut).

Après avoir passé la variable `Ajouter des routes statiques` à `oui` il faut ajouter les paramètres suivants :

- `Adresse IP ou réseau à ajouter dans la table de routage` : permet de définir l'adresse de sous-réseau (ou l'adresse de l'hôte) vers lequel le routage doit s'effectuer ;
- `Masque de sous réseau` : permet de définir le masque du réseau défini ci-dessus (s'il s'agit d'une machine seule, il faut mettre l'adresse du masque à 255.255.255.255) ;

- `Adresse IP de la passerelle pour accéder à ce réseau` : permet de renseigner l'adresse de la passerelle permettant d'accéder au sous-réseau ou à l'hôte défini ci-dessus ;
- `Interface réseau reliée à la passerelle` : permet d'associer la route à une interface donnée. Ce champ, de type liste déroulante, comporte un certain nombre d'interfaces pré-définies. Il est possible d'en ajouter une en tapant son nom (par exemple : `ppp0`) ;
- `Autoriser ce réseau à utiliser les DNS du serveur` : les postes du réseau cible peuvent interroger le service DNS du serveur ;
- `Autoriser ce réseau à utiliser les DNS des zones forward additionnelles` : les postes du réseau cible sont autorisés à interroger les DNS des zones de forward.

Configuration du MTU

La variable `Désactiver le path MTU discovery` permet d'activer ou non le path MTU discovery [p.308] (/proc/sys/net/ipv4/ip_no_pmtu_disc).

Cette option est à `non` par défaut (ip_no_pmtu_disc=0) ce qui est le fonctionnement normal.

Cela peut poser problème, notamment avec le réseau virtuel privé (VPN), lorsque les paquets ICMP[p.306] de type 3 (Destination Unreachable) / code 4 (Fragmentation Needed and Don't Fragment was Set) sont bloqués quelque part sur le réseau.

Un des phénomènes permettant de diagnostiquer un problème lié au PMTU discovery est l'accès à certains sites (ou certaines pages d'un site) n'aboutissant pas (la page reste blanche) ou les courriels n'arrivant pas dans le client de messagerie.

Si vous rencontrez des problèmes d'accès à certains sites (notamment messagerie ou site intranet via le VPN, Gmail ou Gmail Apps), vous pouvez passer ce paramètre à `oui` (ip_no_pmtu_disc=1).

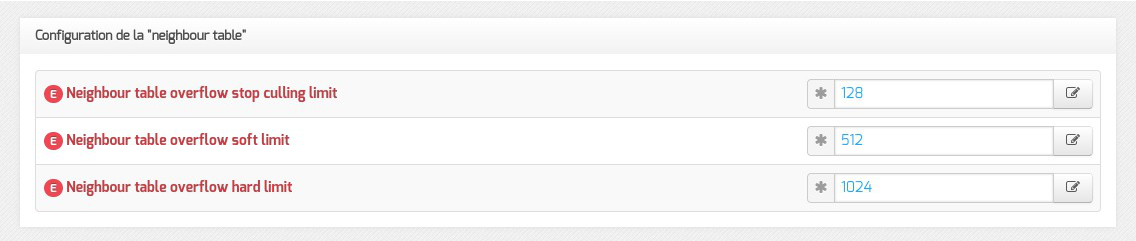
Il est possible de forcer une valeur de MTU[p.308] pour l'interface externe.

Si le champ n'est pas renseigné, la valeur par défaut est utilisée (1500 octets pour un réseau de type Ethernet).

Si l'interface est de type Ethernet et que vous souhaitez forcer une valeur de MTU différente, il faut renseigner le premier champ : `Valeur du MTU pour l'interface eth0`.

Si l'interface est de type PPPoE et que vous souhaitez forcer une valeur de MTU différente, il faut renseigner le second champ : `Valeur du MTU pour l'interface ppp0`.

Configuration de la "neighbour table"



Les variables `ipv4_neigh_default_gc_thresh1`, `ipv4_neigh_default_gc_thresh2` et `ipv4_neigh_default_gc_thresh3` servent à gérer la façon dont la table ARP évolue :

- **gc_thresh1** : seuil en-deçà duquel aucun recyclage des entrées de la table qui ne sont plus utilisées n'est effectué ;
- **gc_thresh2** : seuil qui, s'il est dépassé depuis un certain temps (5 secondes par défaut), déclenche le recyclage des entrées de la table qui ne sont plus utilisées ;
- **gc_thresh3** : seuil au-delà duquel le recyclage est immédiatement déclenché pour contenir la taille de la table.

Test de l'accès distant

Cette variable permet de définir le ou les domaines qui sont utilisés lorsque le module EOLE a besoin de tester son accès à Internet.

En pratique, seul l'accès au premier domaine déclaré est testé sauf dans le cas où il n'est pas accessible.

Les domaines définis sont utilisés dans les outils `diagnose` et dans l'agent Zéphir.

3.11. Onglet Certificats ssl : gestion des certificats SSL

La gestion des certificats a été standardisée pour faciliter leur mise en œuvre.

Ils sont désormais gérés par l'intermédiaire des outils Creole.

Certificats par défaut

Un certain nombre de certificats sont mis en place lors de la mise en œuvre d'un module EOLE :

- `/etc/ssl/certs/ca_local.crt` : autorité de certification propre au serveur (certificats auto-signés) ;
- `/etc/ssl/private/ca.key` : clef privée de la CA ci-dessus ;
- `/etc/ssl/certs/ACInfraEducation.pem` : contient les certificats de la chaîne de certification de l'Éducation nationale (igca/education/infrastructure) ;
- `/etc/ssl/req/eole.p10` : requête de certificat au format pkcs10, ce fichier contient l'ensemble des informations nécessaires à la génération d'un certificat ;
- `/etc/ssl/certs/eole.crt` : certificat serveur généré par la CA locale, il est utilisé par les applications (apache, ead2, eole-sso, ...) ;

- `/etc/ssl/certs/eole.key` : clé du certificat serveur ci-dessus.

Après génération de la CA locale, un fichier `/etc/ssl/certs/ca.crt` est créé qui regroupe les certificats suivants :

- `ca_local.crt` ;
- `ACInfraEducation.pem` ;
- tout certificat présent dans le répertoire `/etc/ssl/local_ca/`

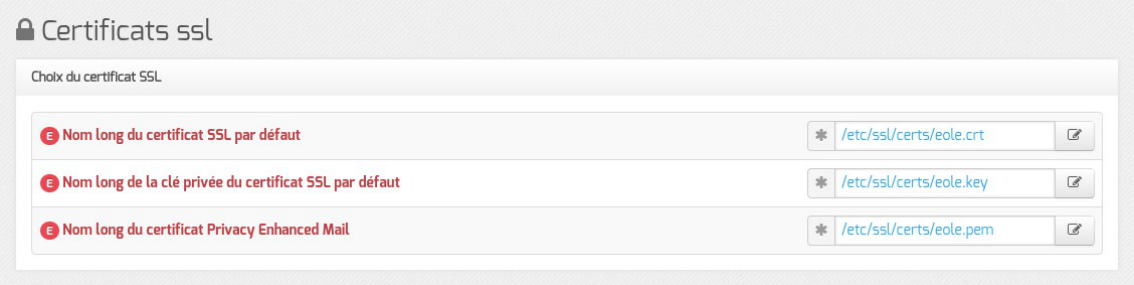
Détermination du nom de serveur (commonName) dans le certificat

Le nom du sujet auquel le certificat s'applique est déterminé de la façon suivante (important pour éviter les avertissements dans les navigateurs) :

- si la variable `ssl_server_name` est définie dans l'interface de configuration du module (onglet `Certifs ssl` -> `Nom DNS du serveur`), elle est utilisée comme nom de serveur dans les certificats ;
- sinon, si un nom de domaine académique est renseigné, le nom sera : `nom_machine.numero_etab.nom_domaine_academique` (exemple : `amon_monetab.0210001A.mon_dom_acad.fr`) ;
- le cas échéant, on utilise : `nom_machine.numero_etab.debut(nom_academie).min(ssl_country_name)` (exemple : `amon_monetab.0210001A.ac-dijon.fr`).

Mise en place d'un certificat particulier

Pour que les services d'un module EOLE utilisent un certificat particulier (par exemple, certificat signé par une autorité tierce), il faut modifier deux variables dans l'onglet `Certificats ssl` de l'interface de configuration du module.



- `Nom long du certificat SSL par défaut` (server_cert) : chemin d'un certificat au format PEM à utiliser pour les services ;
- `Nom long de la clé privée du certificat SSL par défaut` (server_key) : chemin de la clé privée correspondante (éventuellement dans le même fichier).

Dans le cas d'un certificat signé par une autorité externe, copier le certificat de la CA en question dans `/etc/ssl/local_ca/` pour qu'il soit pris en compte automatiquement (non nécessaire pour les certificats de l'IGC nationale).

Le répertoire `/etc/ssl/certs/` accueille le fichier de certificat issu de la CA interne ainsi que la clé privée correspondant au certificat.

Il faut déclarer les bons chemins dans l'interface de configuration du module.

Pour appliquer les modifications, utilisez la commande `reconfigure`.

Si les certificats configurés ne sont pas trouvés, ils sont générés à partir de la CA locale.

Le répertoire `/etc/ssl/local_ca/` n'accueille que des certificats CA.

Création de nouveaux certificats

Le script `/usr/share/creole/gen_certif.py` permet de générer rapidement un nouveau certificat SSL.

Génération d'un certificat avec gen_certif.py

```
root@eole:~#          /usr/share/creole/gen_certif.py          -fc
/etc/ssl/certs/test.crt
Generation du certificat machine
* Certificat /etc/ssl/certs/test.crt généré
```

Obtention d'un certificat signé par l'IGC de l'Éducation nationale

Étapes à suivre :

1. récupérer la requête du certificat située dans le répertoire `/etc/ssl/req/` : `eole.p10` ;
2. se connecter sur l'interface web de demande des certificats et suivre la procédure ;
3. récupérer le certificat depuis l'interface (copier/coller dans un fichier) ;
4. copier le fichier dans le répertoire `/etc/ssl/certs/`.

Seuls les ISR/OSR des académies sont accrédités pour effectuer les demandes.

Certificats intermédiaires

En attendant que la prise en compte des certificats intermédiaires soit automatisée pour l'ensemble des services de base (fixme #13362 [https://dev-eole.ac-dijon.fr/issues/13362]), les manipulations nécessaires pour éviter des avertissements dans les navigateurs sont documentées dans la page wiki suivante : https://dev-eole.ac-dijon.fr/projects/modules-eole/wiki/Gestion_certificats

3.12. Onglet Agrégation : Mise en place d'une répartition de charge ou d'une haute disponibilité

Présentation et mise en place de l'agrégation de liens

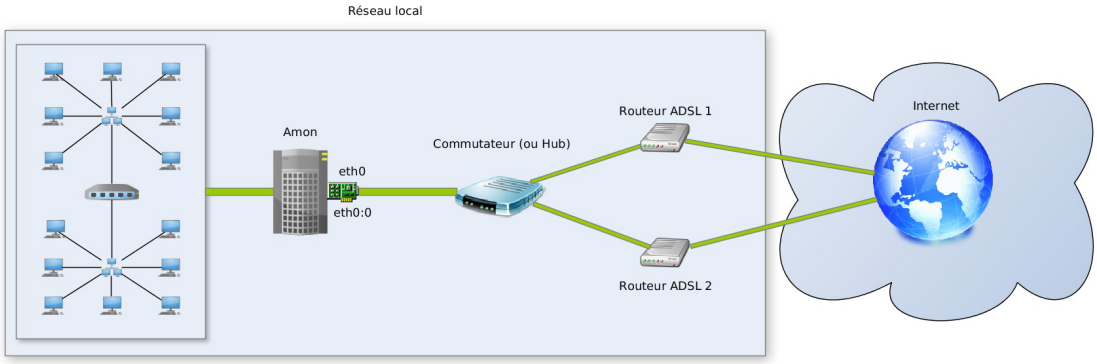
L'agrégation de liens permet la mise en place d'une répartition de charge ou d'une haute disponibilité pour les sorties Internet.

Les deux routeurs sont reliés entre eux par un commutateur (ou un Hub) à la carte eth0 du module Amon.

Dans ce cas :

- pas besoin d'utiliser les protocoles d'annonce de routes RIP[p.312] et OSPF[p.310] ;

- il faut un service qui surveille l'état de chacun des liens.



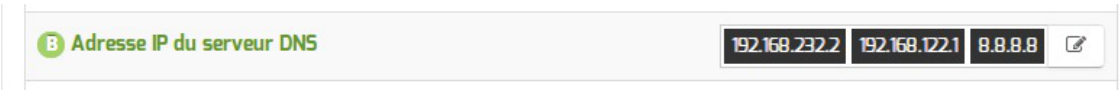
Il est nécessaire d'activer un alias sur l'interface réseau connectée sur l'extérieur pour utiliser ce service.

La configuration de l'agrégation est le résultat de plusieurs contributions de collègues en académie.

La première version a été réalisée par l'académie de Versailles, puis elle a été améliorée successivement par les académies de Nantes et de Lyon.

Onglet Général

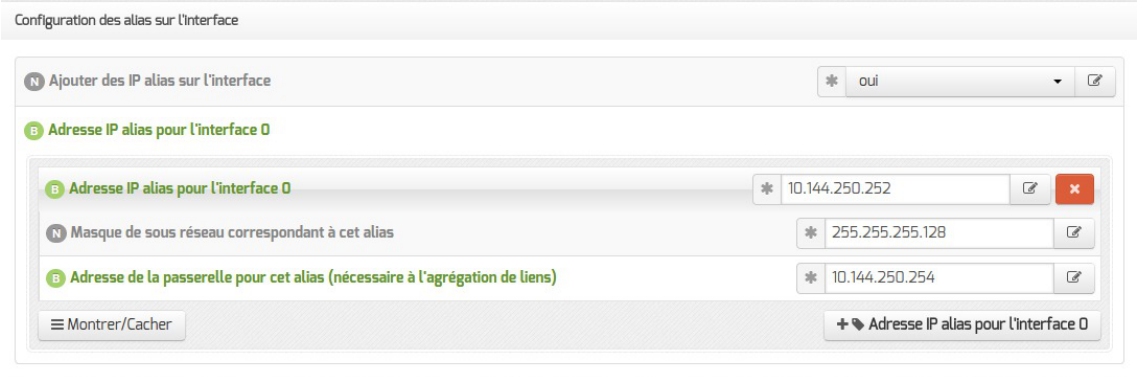
Dans la section `Adresse IP du serveur DNS` de l'onglet Général, ajouter les adresses des serveurs DNS de chacun des fournisseurs, en plaçant, de préférence, le DNS du premier lien en première position.



Onglet Interface-0

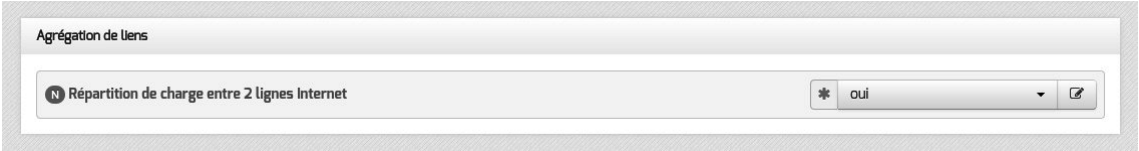
Il faut, en premier lieu, déclarer un alias sur l'interface eth0 dans la section `Configuration des alias sur l'interface`.

Les paramètres réseaux (IP, masque et passerelle) doivent être ceux attribués par le fournisseur d'accès du second lien.



Création d'un alias sur eth0 pour l'agrégation de liens

L'activation d'un alias IP, fait apparaître un nouveau paramètre, `Répartition de charge entre 2 lignes Internet`, qu'il faut passer à `oui`.

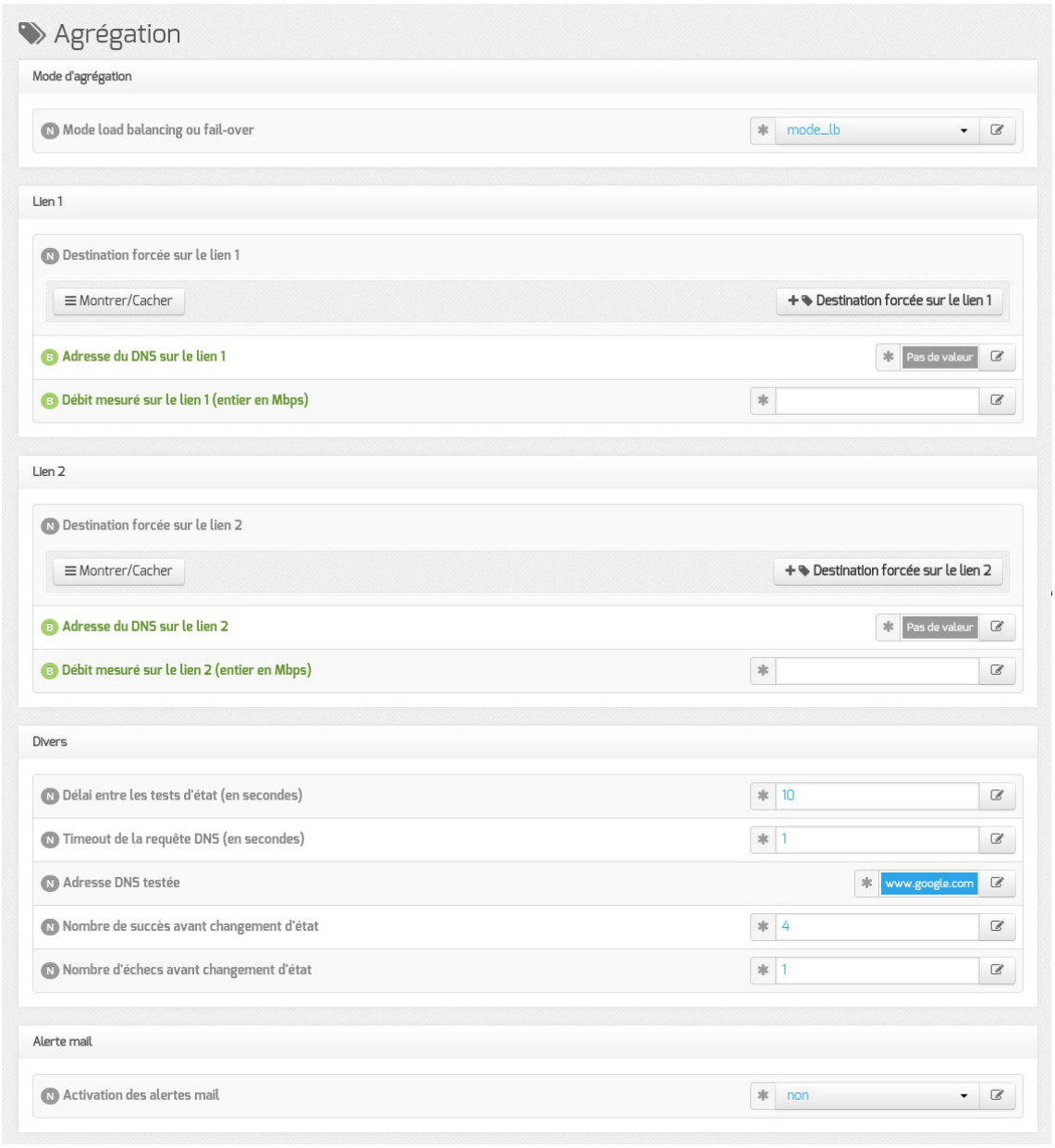


Activation de l'agrégation de lien

Un nouvel onglet, `Agrégation`, est disponible.

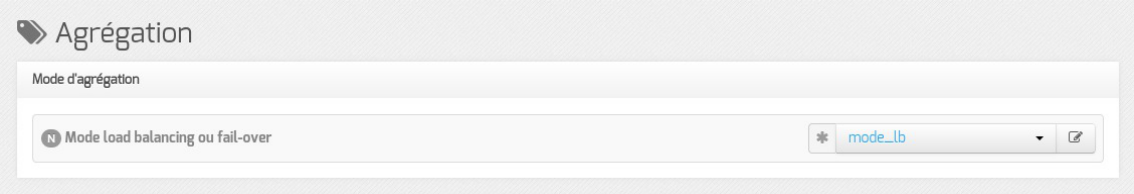
Onglet Agrégation : Configuration de l'agrégation de liens

Pour avoir accès à l'onglet concernant l'agrégation, il faut avoir activé la `Répartition de charge entre 2 lignes Internet` dans l'onglet `Interface-0` comme expliqué précédemment.



Paramétrage de l'agrégation de liens

Modes d'agrégation



Il existe deux modes d'agrégation :

- le mode `mode-lb` (pour load balancing) correspond à la répartition de charge et fonctionne avec la notion de poids à utiliser sur les différentes passerelles ;
- le mode `mode-fo`, (pour fail-over) un seul lien est utilisé à la fois, il n'y a plus de notion de poids et il n'y a plus qu'une seule route par défaut.

Dans les deux modes il est possible de forcer des destinations IP ou réseau, et dans les deux cas si un lien tombe tous les flux (et également les destinations forcées) sont redirigés vers le second lien.

Quand les deux liens sont fonctionnels, on se retrouve dans la configuration de départ.

Le VPN, de par son mode de fonctionnement, ne peut pas être réparti entre plusieurs abonnements.

Tout le trafic devant passer par un seul lien, il est nécessaire d'utiliser le mécanisme de destination forcée.

Que le `Lien 1` ou le `Lien 2` soit choisi pour faire transiter le VPN, s'il devient indisponible, le VPN ne fonctionnera plus.

Adresse des DNS

Les champs `Adresse du DNS sur le lien 1` et `Adresse du DNS sur le lien 2` sont des champs obligatoires pour le bon fonctionnement de l'agrégation.

Les adresses DOIVENT être différentes sur chaque lien car c'est avec ces DNS que se font les tests d'état des liens.

Adresse DNS testée

Il est possible de spécifier plusieurs mires de tests qui seront testées afin de déterminer l'état des liens (résolution DNS avec le serveur DNS de chacun des liens).

L'ensemble des DNS doit être déclaré dans l'onglet `Général`.

Alerte mail

Lorsque l'un des liens est coupé, le message suivant est envoyé : `Seul le lien 2 est actif, redirection des flux sur ce lien`.

Quand les deux liens sont de nouveaux fonctionnels, le message suivant est envoyé : `Rechargement de la répartition sur les 2 liens`.

3.13. Onglet Clamav : Configuration de l'anti-virus

EOLE propose un service anti-virus réalisé à partir du logiciel libre Clamav.

http://www.clamav.net

Activation de l'anti-virus

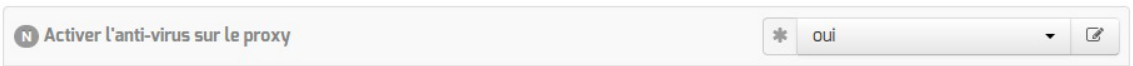
L'onglet `Clamav` n'est accessible que si le service est activé dans l'onglet `Services`. Pour ce faire, passer la variable `Activer l'anti-virus ClamAV` à `oui`.

Sur le module Amon, il n'est possible d'activer l'anti-virus que sur le proxy et sur la messagerie.

Si aucun service n'utilise l'anti-virus, il est utile de le désactiver dans l'onglet `Services`. Il faut passer la variable `Activer l'anti-virus ClamAV` à `non`. L'onglet `Clamav` n'est alors plus visible.

Activation de l'anti-virus sur le proxy

Pour activer l'anti-virus en temps réel sur les fichiers filtrés par le proxy Internet, il faut passer la variable `Activer l'anti-virus sur le proxy` à `oui` dans l'onglet `Clamav`.

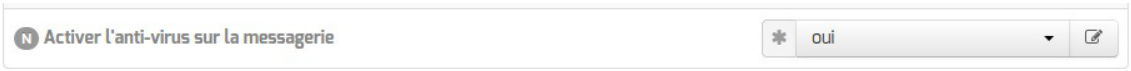


L'anti-virus sur le proxy permet d'analyser le trafic HTTP mais ne saurait en aucun cas remplacer la présence d'un anti-virus sur les postes clients.

> L'anti-virus activé sur le proxy utilise beaucoup de ressources CPU[p.303]. Il peut donc affecter les performances du pare-feu et considérablement ralentir la navigation.

Activation de l'anti-virus sur la messagerie

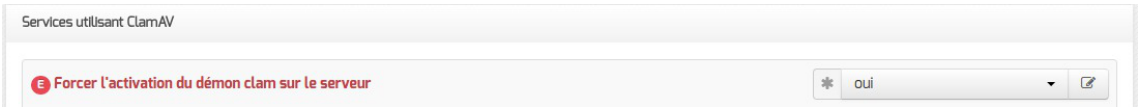
Pour activer l'anti-virus sur la messagerie il faut passer la variable `Activer l'antivirus sur la messagerie` à `oui` dans l'onglet `Clamav`.



Forcer l'activation du service clamd

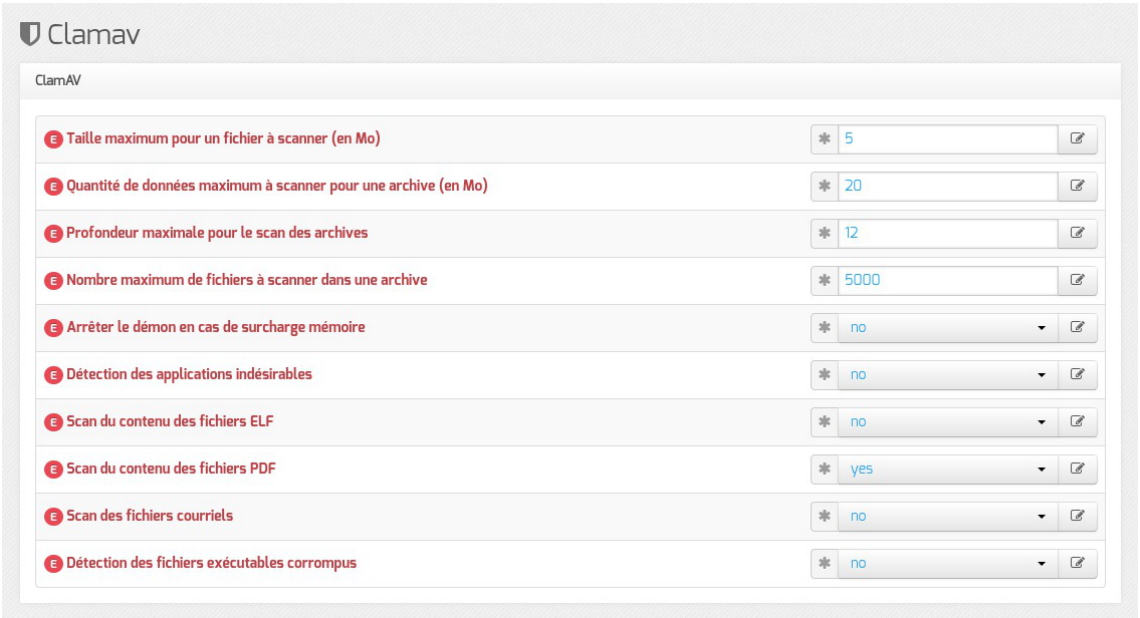
Si `Activer l'anti-virus ClamAV` est à `oui` dans l'onglet `Service` mais qu'aucun service EOLE ne l'utilise alors seul le service de mise à jour de la base de signatures (freshclam) sera actif sur le serveur.

À partir de la version 2.5.2 d'EOLE, il est possible de forcer l'activation du service anti-virus (clamd) en passant la variable du mode expert `Forcer l'activation du démon clam sur le serveur` à `oui` dans l'onglet `Clamav`.



Configuration avancée

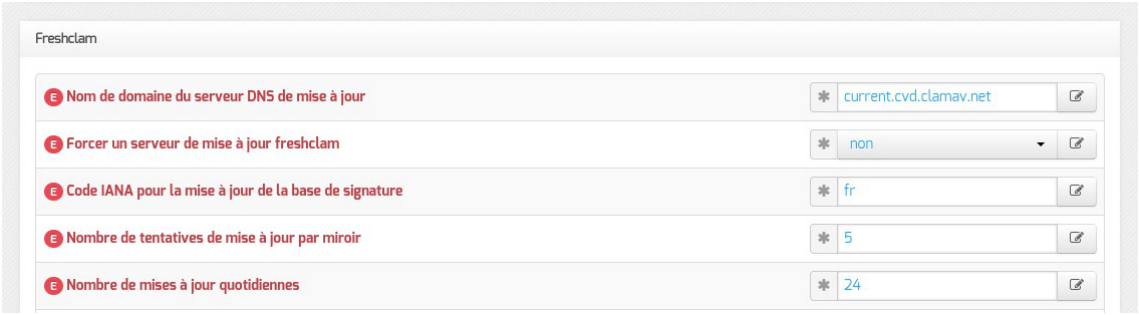
En mode expert, l'onglet `Clamav` comporte de nombreuses variables qui permettent d'affiner la configuration de ClamAV.



- `Taille maximum pour un fichier à scanner (en Mo)` ;
- `Quantité de données maximum à scanner pour une archive (en Mo)` ;
- `Profondeur maximale pour le scan des archives` ;

- `Nombre maximum de fichiers à scanner dans une archive` ;
- `Arrêter le démon en cas de surcharge mémoire` ;
- `Détection des applications indésirables` ;
- `Scan du contenu des fichiers ELF` [p.305] *[p.305] ;
- `Scan du contenu des fichiers PDF` ;
- `Scan des fichiers courriels` ;
- `Détection des fichiers exécutables corrompus`.

En mode expert, l'onglet `Clamav` comporte des variables qui permettent d'affiner la configuration de Freshclam, le service de mise à jour de la base de signatures.



- `Nom de domaine du serveur DNS de mise à jour` permet de spécifier un miroir interne pour les signatures ;
- `Forcer un serveur de mise à jour freshclam` permet d'ajouter un ou plusieurs miroirs pour les signatures ;
- `Code IANA pour la mise à jour de la base de signature` ;
- `Nombre de tentatives de mise à jour par miroir` permet de réduire le nombre de tentatives de mise à jour, en effet des fichiers sont récupérés systématiquement à chaque tentative ;
- `Nombre de mises à jour quotidiennes` permet de réduire le nombre de mises à jour quotidiennes.

Contribuer

La base de données de virus est mise à jour avec l'aide de la communauté.

Il est possible de faire des signalements :

- signaler de nouveaux virus qui ne sont pas détectés par ClamAV ;
- signaler des fichiers propres qui ne sont pas correctement détectés par ClamAV (faux-positif).

Pour cela il faut utiliser le formulaire suivant (en) : http://cgi.clamav.net/sendvirus.cgi

L'équipe de ClamAV examinera votre demande et mettra éventuellement à jour la base de données.

En raison d'un nombre élevé de déposants, il ne faut pas soumettre plus de deux fichiers par jour.

Il ne faut pas signaler des PUA[p.312] comme étant des faux positifs.

3.14. Onglet Relai DHCP

Pour des raisons de sécurité, le service DHCP[p.303] n'a pas, à priori, à être installé sur le module Amon.

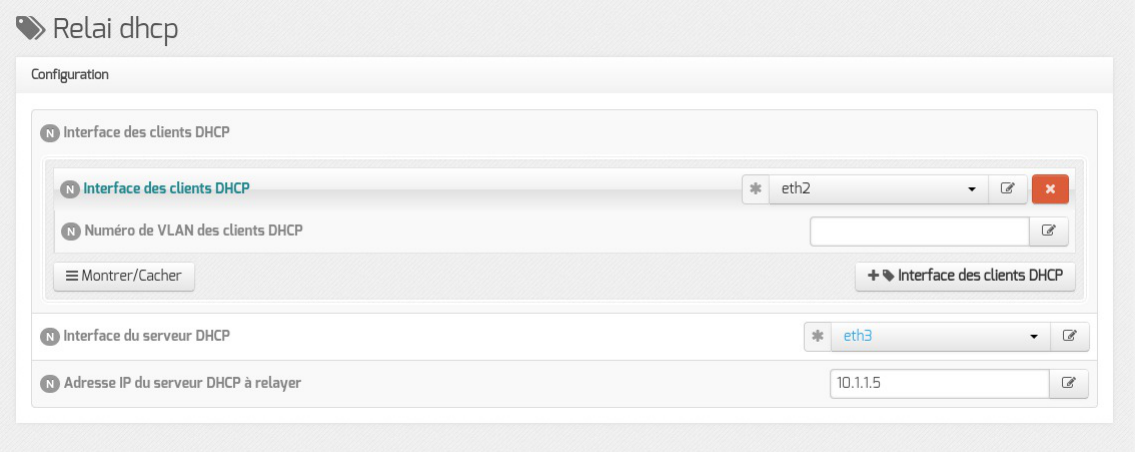
Il vaut mieux utiliser un autre module (module Scribe ou module Horus par exemple) pour fournir ce service.

Le protocole DHCP fonctionne en utilisant un mécanisme de broadcast[p.302].

De ce fait, les trames ne sont, par défaut, pas routables d'un réseau vers un autre.

Si le serveur DHCP ne se situe pas sur la même zone que les stations, il faut mettre en place un relai DHCP.

L'onglet `Relai dhcp` n'est accessible que si le service est activé dans l'onglet `Services`. Pour ce faire, passer la variable `Activer le relai DHCP` à `oui`.



Vue de l'onglet Relai dhcp de l'interface de configuration du module

Dans la configuration ci-dessus (4zones), on déclare que l'on veut relayer le DHCP du module Scribe (adresse IP : 10.1.1.5) qui se trouve dans la DMZ (eth3 est la 4ème interface) vers le réseau pédagogique (eth2 est la 3ème interface).

Il est possible de restreindre le relayage sur un VLAN[p.314] particulier en renseignant son numéro dans la variable `Numéro de VLAN des clients DHCP`.

Grâce au découpage des paquets par services, la mise en œuvre d'un DHCP sur le module Amon, bien que déconseillée, est facilitée par le paquet `eole-dhcp`.

Voir aussi...

eole-dhcp

Configuration du module Amon avec le module Scribe en DMZ [p.187]

3.15. Onduleur

Sur chaque module EOLE, il est possible de configurer votre onduleur.

Le logiciel utilisé pour la gestion des onduleurs est NUT[p.309]. Il permet d'installer plusieurs clients sur le

même onduleur. Dans ce cas, une machine aura le contrôle de l'onduleur (le maître/master) et en cas de coupure, lorsque la charge de la batterie devient critique, le maître indiquera aux autres machines (les esclaves) de s'éteindre avant de s'éteindre lui-même.

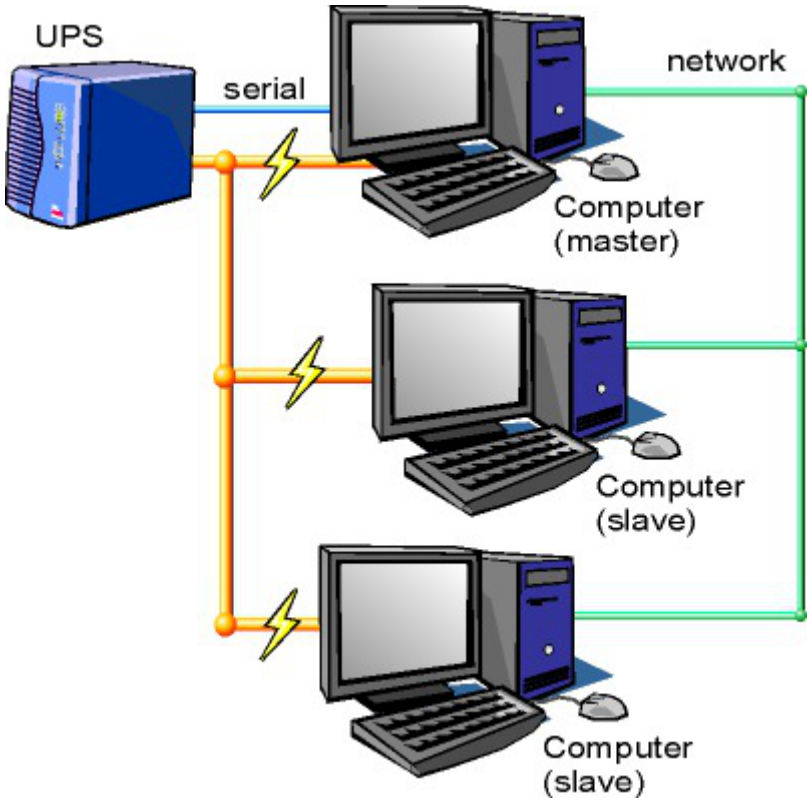


Schéma d'Olivier Van Hoof sous licence GNU FDL Version 1.2 - http://ovanhoof.developpez.com/upsusb/

Certains onduleurs sont assez puissants pour alimenter plusieurs machines.

http://www.networkupstools.org/

Le projet offre une liste de matériel compatible avec le produit mais cette liste est donnée pour la dernière version du produit :

http://www.networkupstools.org/stable-hcl.html

Pour connaître la version de NUT qui est installée sur le module :

```
# apt-cache policy nut
```

ou encore :

```
# apt-show-versions nut
```

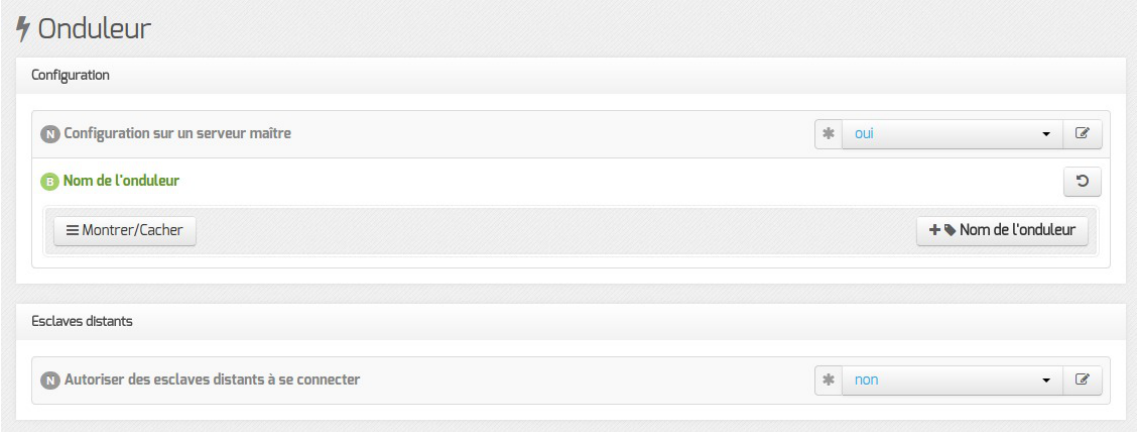
Si la version retournée est 2.7.1 on peut trouver des informations sur la prise en charge du matériel dans les notes de version à l'adresse suivante :

http://www.networkupstools.org/source/2.7/new-2.7.1.txt

Si le matériel n'est pas dans la liste, on peut vérifier que sa prise en charge soit faite par une version plus récente et donc non pris en charge par la version actuelle :

http://www.networkupstools.org/source/2.7/new-2.7.3.txt

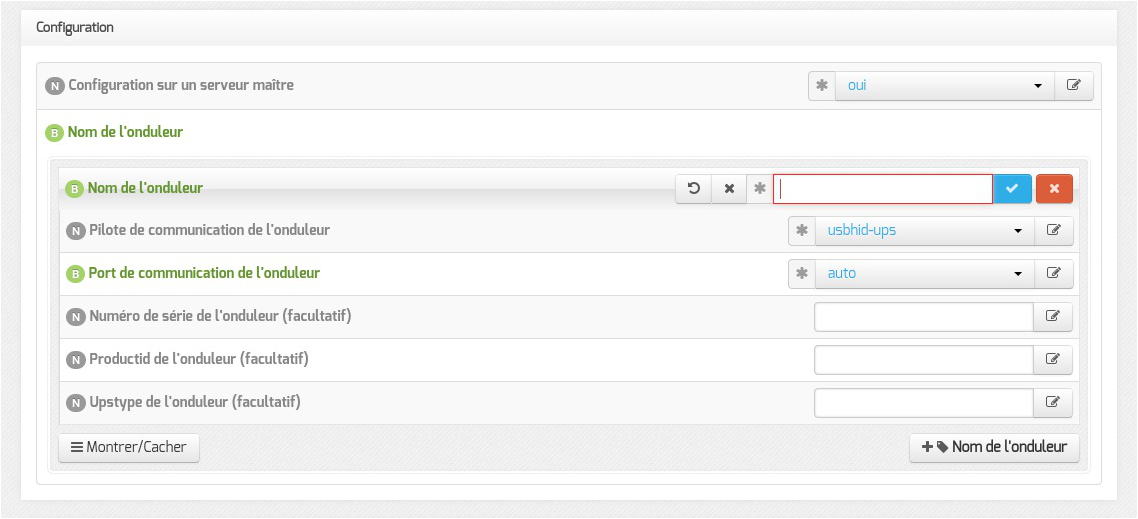
L'onglet `Onduleur` n'est accessible que si le service est activé dans l'onglet `Services`.



Vue de l'onglet Onduleur

Si l'onduleur est branché directement sur le module il faut laisser la variable `Configuration sur un serveur maître` à `oui`, cliquer sur le bouton `+ Nom de l'onduleur` et effectuer la configuration liée au serveur maître.

La configuration sur un serveur maître



Même si le nom de l'onduleur n'a aucune conséquence, il est obligatoire de remplir cette valeur dans le champ `Nom pour l'onduleur`.

Il faut également choisir le nom du pilote de l'onduleur dans la liste déroulante `Pilote de communication de l'onduleur` et éventuellement préciser le `Port de communication` si l'onduleur n'est pas USB.

Les champs `Numéro de série de l'onduleur`, `Productid de l'onduleur` et `Upstype de l'onduleur` sont facultatifs si il n'y a pas de serveur esclave. Il n'est nécessaire d'indiquer ce numéro de série que dans le cas où le serveur dispose de plusieurs onduleurs et de serveurs esclaves.

Le nom de l'onduleur ne doit contenir que des chiffres ou des lettres en minuscules : *[a-z][0-9]* sans espaces, ni caractères spéciaux.

Configuration d'un second onduleur sur un serveur maître

Si le serveur dispose de plusieurs alimentations, il est possible de les connecter chacune d'elle à un onduleur différent.

Il faut cliquer sur le bouton `+ Nom de l'onduleur` pour ajouter la prise en charge d'un onduleur supplémentaire dans l'onglet `Onduleur` de l'interface de configuration du module.

Si les onduleurs sont du même modèle et de la même marque, il faut ajouter de quoi permettre au pilote NUT de les différencier.

Cette différenciation se fait par l'ajout d'une caractéristique unique propre à l'onduleur. Ces caractéristiques dépendent du pilote utilisé, la page de `man` du pilote vous indiquera lesquelles sont disponibles.

Exemple pour le pilote Solis :

```
# man solis
```

Afin de récupérer la valeur il faut :

- ne connecter qu'un seul des onduleurs ;
- le paramétrer comme indiqué dans la section précédente ;
- exécuter la commande : `upsc <nomOnduleurDansGenConfig>@localhost|grep <nom_variable>` ;
- débrancher l'onduleur ;
- brancher l'onduleur suivant ;
- redémarrer `nut` avec la commande : `# service nut restart` ;
- exécuter à nouveau la commande pour récupérer la valeur de la variable.

Une fois les numéros de série connus, il faut les spécifier dans les champ `Numéro de série de l'onduleur` de chaque onduleur.

Deux onduleurs de même marque

Pour deux onduleurs de marque MGE, reliés à un module Scribe par câble USB, il est possible d'utiliser la valeur "serial", voici comment la récupérer :

```
# upsc <nomOnduleurDansGenConfig>@localhost | grep serial
driver.parameter.serial: AV4H4601W
ups.serial: AV4H4601W
```

Deux onduleurs différents

Un onduleur sur port série :

- Nom de l'onduleur : `eoleups` ;
- Pilote de communication de l'onduleur : `apcsmart` ;
- Port de communication de l'onduleur : `/dev/ttyS0`.

Si l'onduleur est branché sur le port série (en général : `/dev/ttyS0`), les droits doivent être adaptés.

Cette adaptation est effectuée automatiquement lors de l'application de la configuration.

Onduleur sur port USB :

- Nom de l'onduleur : `eoleups` ;

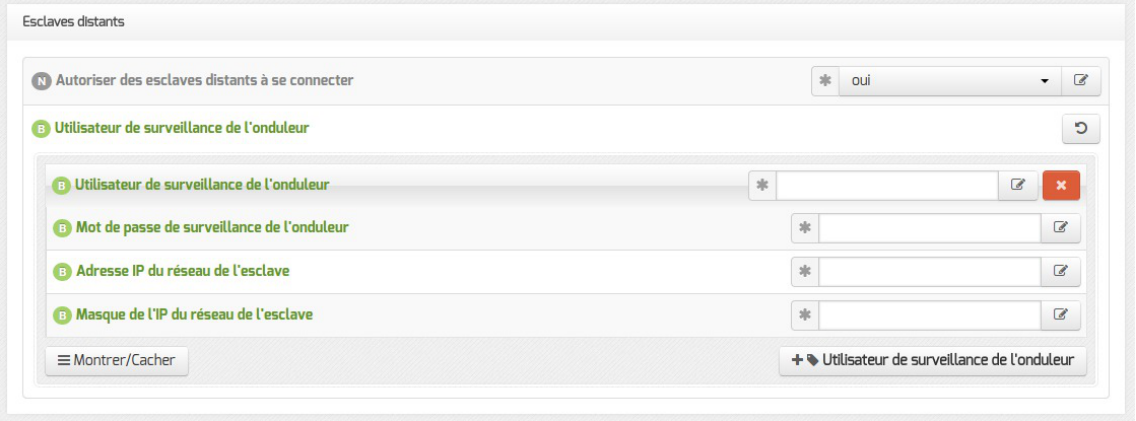
- Pilote de communication de l 'onduleur : `usbhid-ups` ;
- Port de communication de l'onduleur : `auto`.

La majorité des onduleurs USB sont détectés automatiquement.

Attention, seul le premier onduleur sera surveillé.

Autoriser des esclaves distants à se connecter

Pour déclarer un serveur esclave, il faut passer la variable `Autoriser des esclaves distants à se connecter` à `oui` puis ajouter un utilisateur sur le serveur maître afin d'autoriser l'esclave a se connecter avec cet utilisateur.



Idéalement, il est préférable de créer un utilisateur différent par serveur même s'il est possible d'utiliser un unique utilisateur pour plusieurs esclaves. Pour configurer plusieurs utilisateurs il faut cliquer sur le bouton `+ Utilisateur de surveillance de l'onduleur`.

Pour chaque utilisateur, il faut saisir :

- un `Utilisateur de surveillance de l'onduleur` ;
- un `Mot de passe de surveillance de l'onduleur` associé à l'utilisateur précédemment créé ;
- l'`Adresse IP du réseau de l'esclave` (cette valeur peut être une adresse réseau plutôt qu'une adresse IP) ;
- le `Masque de l'IP du réseau de l'esclave` (comprendre le masque du sous réseau de l'adresse IP de l'esclave)

Le nom de l'onduleur ne doit contenir que des chiffres ou des lettres en minuscules : *[a-z][0-9]* sans espaces, ni caractères spéciaux.

Chaque utilisateur doit avoir un nom différent.

Les noms `root` et `localmonitor` sont réservés.

Pour plus d'informations, vous pouvez consulter la page de manuel : `man ups.conf` ou consulter la page web suivante : http://manpages.ubuntu.com/manpages/trusty/en/man5/ups.conf.5.html

Configurer un serveur esclave

Une fois qu'un serveur maître est configuré et fonctionnel, il est possible de configurer le ou les serveurs esclaves.

Pour configurer le module en tant qu'esclave, il faut activer le service dans l'onglet `Services` puis, dans l'onglet `Onduleur`, passer la variable `Configuration sur un serveur maître` à `non`.

Il faut ensuite saisir les paramètres de connexion à l'hôte distant :

- le `Nom de l'onduleur distant` (valeur renseignée sur le serveur maître) ;
- l'`Hôte gérant l'onduleur` (adresse IP ou nom d'hôte du serveur maître) ;
- l'`Utilisateur de l'hôte distant` (nom d'utilisateur de surveillance créé sur le serveur maître) ;
- le `Mot de passe de l'hôte distant` (mot de passe de l'utilisateur de surveillance créé sur le serveur maître).

Exemple de configuration

Sur le serveur maître :

- Nom de l'onduleur : `eoleups` ;
- Pilote de communication de l'onduleur : `usbhid-ups` ;
- Port de communication de l'onduleur : `auto` ;
- Utilisateur de surveillance de l'onduleur : `scribe` ;
- Mot de passe de surveillance de l'onduleur : `99JJUE2EZOAI2IZI10IIZ93I187UZ8` ;
- Adresse IP du réseau de l'esclave : `192.168.30.20` ;
- Masque de l'IP du réseau de l'esclave : `255.255.255.255`.

Sur le serveur esclave :

- Nom de l'onduleur distant : `eoleups` ;
- Hôte gérant l'onduleur : `192.168.30.10` ;
- Utilisateur de l'hôte distant : `scribe` ;
- Mot de passe de l'hôte distant : `99JJUE2EZOAI2IZI10IIZ93I187UZ8`.

3.16. Onglet Eole sso : Configuration du service SSO pour l'authentification unique

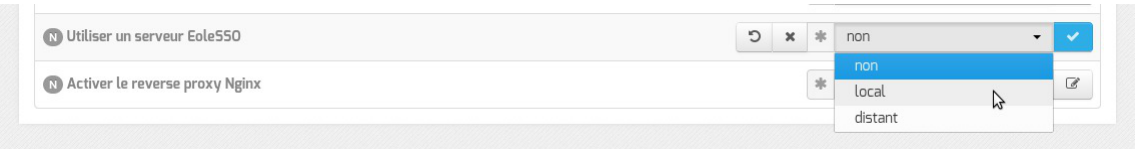
Le serveur EoleSSO est prévu pour être déployé sur un module EOLE.

Il est cependant possible de l'utiliser dans un autre environnement en modifiant manuellement le fichier de configuration `/usr/share/sso/config.py`.

Cette section décrit la configuration du serveur depuis l'interface de configuration du module disponible sur tous les modules EOLE. Les valeurs définies par défaut simplifient la configuration dans le cadre d'une utilisation prévue sur les modules EOLE.

Serveur local ou distant

L'activation du serveur EoleSSO s'effectue dans l'onglet `Services`.



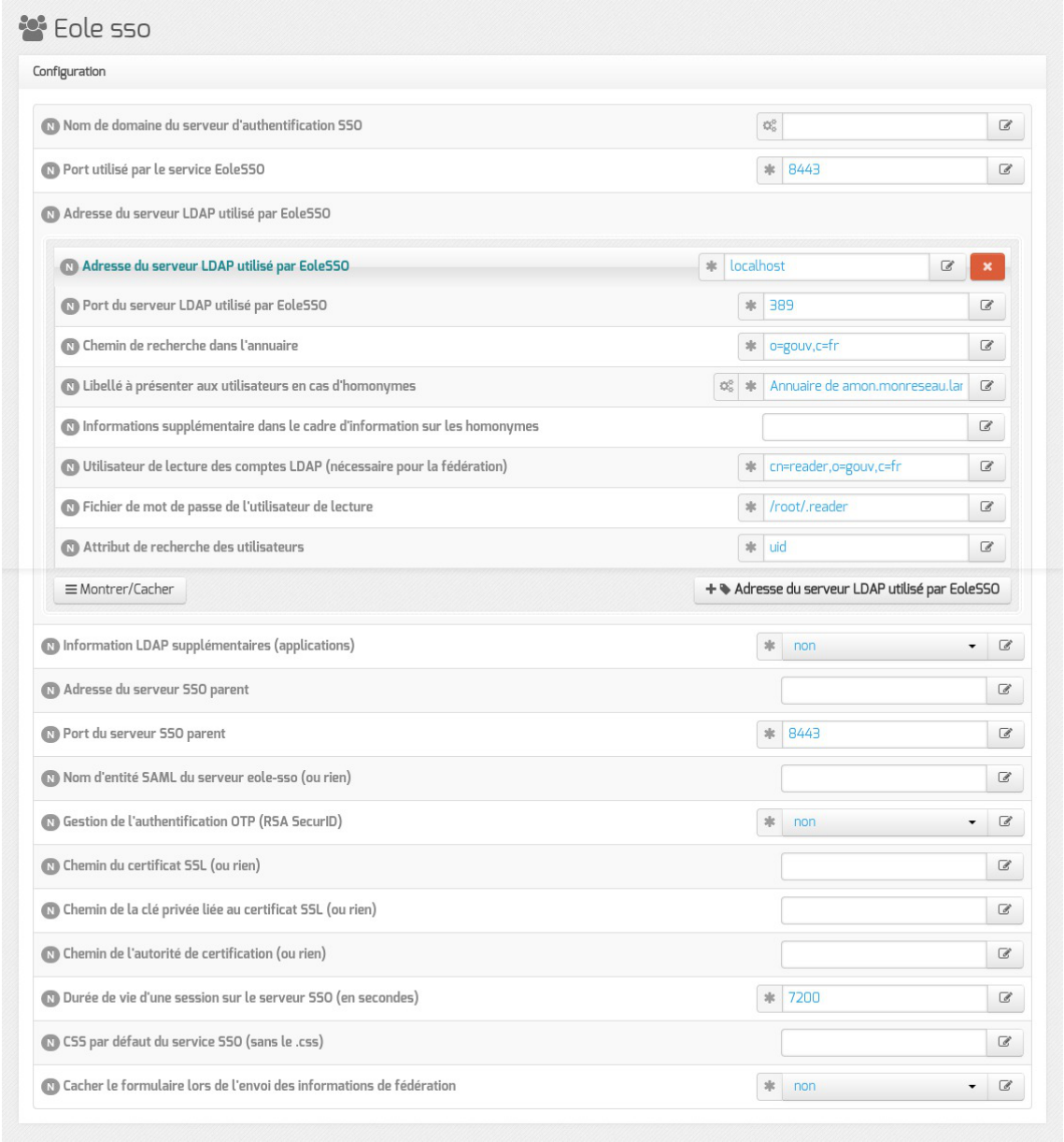
Activation du serveur SSO dans l'interface de configuration du module

La variable `Utiliser un serveur EoleSSO` permet :

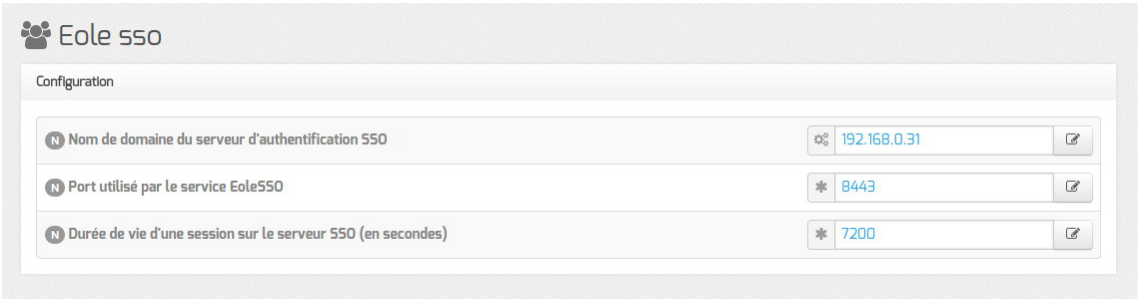
- `non` : de ne pas utiliser de SSO sur le serveur ;
- `local` : d'utiliser et de configurer le serveur EoleSSO local ;
- `distant` : d'utiliser un serveur EoleSSO distant (configuration cliente).

Adresse et port d'écoute

L'onglet supplémentaire `Eole-sso` apparaît si l'on a choisi d'utiliser un serveur EoleSSO local ou distant.



Dans le cas de l'utilisation d'un serveur EoleSSO distant, seuls les paramètres `Nom de domaine du serveur d'authentification SSO` et `Port utilisé par le service EoleSSO` sont requis et les autres options ne sont pas disponibles car elles concernent le paramétrage du serveur local.



Dans le cas de l'utilisation du serveur EoleSSO local, `Nom de domaine du serveur d'authentification SSO` doit être renseigné avec le nom DNS du serveur.

Par défaut le serveur communique sur le port `8443`. Il est conseillé de laisser cette valeur

par défaut en cas d'utilisation avec d'autres modules EOLE.

Si vous décidez de changer ce port, pensez à le changer également dans la configuration des autres machines l'utilisant.

Configuration LDAP

Le serveur EoleSSO se base sur des serveurs LDAP pour authentifier les utilisateurs et récupérer leurs attributs.

Il est possible ici de modifier les paramètres d'accès à ceux-ci :

- l'adresse et le port d'écoute du serveur LDAP ;
- le chemin de recherche correspond à l'arborescence de base dans laquelle rechercher les utilisateurs ;
- un libellé à afficher dans le cas où un utilisateur aurait à choisir entre plusieurs annuaires/établissements pour s'authentifier (voir le chapitre `Gestion des sources d'authentifications multiples`) ;
- un fichier d'informations à afficher dans le cadre qui est présenté en cas d'homonymes. Ces informations apparaîtront si l'utilisateur existe dans l'annuaire correspondant. Les fichiers doivent être placés dans le répertoire `/usr/share/sso/interface/info_homonymes` ;
- DN et mot de passe d'un utilisateur en lecture pour cet annuaire ;
- attribut de recherche des utilisateurs : indique l'attribut à utiliser pour rechercher l'entrée de l'utilisateur dans l'annuaire (par défaut, uid)
- choix de la disponibilité ou non de l'authentification par clé OTP[p.310] si disponible *(voir plus loin)*.

Dans le cas où vous désirez fédérer EoleSSO avec d'autres fournisseurs de service ou d'identité (ou 2 serveurs EoleSSO entre eux), il est nécessaire de configurer un utilisateur ayant accès en lecture au serveur LDAP configuré.

Il sera utilisé pour récupérer les attributs des utilisateurs suite à réception d'une assertion d'un fournisseur d'identité (ou dans le cas d'une authentification par OTP).

Cet utilisateur est pré-configuré pour permettre un accès à l'annuaire local sur les serveurs EOLE.

Sur les modules EOLE, la configuration recommandée est la suivante :

- utilisateur : `cn=reader,o=gouv,c=fr`
- fichier de mot de passe : `/root/.reader`

Si vous connectez EoleSSO à un annuaire externe, vous devez définir vous même cet utilisateur :

- `Utilisateur de lecture des comptes ldap` : renseignez son *dn* complet dans l'annuaire
- `fichier de mot de passe de l'utilisateur de lecture` : entrez le chemin d'un fichier ou vous stockerez son mot de passe (modifiez les droits de ce fichier pour qu'il soit seulement accessible par l'utilisateur `root`)

Serveur SSO parent

Un autre serveur EoleSSO peut être déclaré comme serveur parent dans la configuration (adresse et port). Se reporter au chapitre traitant de la fédération pour plus de détails sur cette notion.

Si un utilisateur n'est pas connu dans le référentiel du serveur EoleSSO, le serveur essayera de l'authentifier auprès de son serveur parent (dans ce cas, la liaison entre les 2 serveurs se fait par l'intermédiaire d'appels XML-RPC[p.315] en HTTPS, sur le port défini pour le serveur EoleSSO).

Si le serveur parent authentifie l'utilisateur, il va créer un cookie de session local et rediriger le navigateur client sur le serveur parent pour qu'une session y soit également créée (le cookie de session est accessible seulement par le serveur l'ayant créé).

Ce mode de fonctionnement n'est plus recommandé aujourd'hui. Il faut préférer à cette solution la mise en place d'une fédération par le protocole SAML.

Prise en compte de l'authentification OTP

Il est possible de configurer EoleSSO pour gérer l'authentification par clé OTP à travers le protocole securID[p.312] de la société EMC (précédemment RSA).

Pour cela il faut :

- installer et configurer le client PAM/Linux proposé par EMC (voir annexes)
- Répondre `oui` à la question `Gestion de l'authentification OTP (RSA SecurID)`

Des champs supplémentaires apparaissent :

- Pour chaque annuaire configuré, un champ permet de choisir la manière dont les identifiants à destination du serveur OTP sont gérés. '`inactifs`' (par défaut) indique que l'authentification OTP n'est pas proposée à l'utilisateur. Avec `'identiques'`, le login local (LDAP) de l'utilisateur sera également utilisé comme login OTP. La dernière option est '`configurables`', et indique que les utilisateurs doivent renseigner eux même leur login OTP. Dans ce dernier cas, l'identifiant est conservé sur le serveur EoleSSO pour que l'utilisateur n'ait pas à le renseigner à chaque fois (fichier `/usr/share/sso/securid_users/securid_users.ini`).
- Le formulaire d'authentification détecte automatiquement si le mot de passe entré est un mot de passe OTP. Il est possible de modifier la reconnaissance si elle ne convient pas en réglant les tailles minimum et maximum du mot de passe et en donnant une expression régulière qui sera vérifiée si la taille correspond. Les options par défaut correspondent à un mot de passe de 10 à 12 caractères uniquement numériques.

Certificats

Les communications de et vers le serveur EoleSSO sont chiffrées.

Sur les modules EOLE, des certificats auto-signés sont générés à l'instanciation[p.306] du serveur et sont utilisés par défaut.

Il est possible de renseigner un chemin vers une autorité de certification et un certificat serveur dans le cas de l'utilisation d'autres certificats (par exemple, des certificat signés par une entité reconnue).

Les certificats doivent être au format PEM.

Fédération d'identité

Le serveur EoleSSO permet de réaliser une fédération vers un autre serveur EoleSSO ou vers d'autre types de serveurs compatibles avec le protocole SAML[p.312] (version 2).

`Nom d'entité SAML du serveur eole-sso (ou rien)` : nom d'entité du serveur EoleSSO local à indiquer dans les messages SAML. Si le champ est laissé à vide, une valeur est calculée à partir du nom de l'académie et du nom de la machine.

`Cacher le formulaire lors de l'envoi des informations de fédération` : permet de ne pas afficher le formulaire de validation lors de l'envoi des informations de fédération à un autre système. Ce formulaire est affiché par défaut et indique la liste des attributs envoyés dans l'assertion SAML permettant la fédération.

Autres options

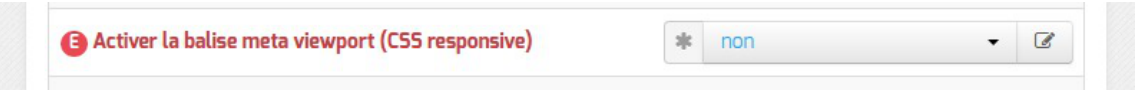
`Durée de vie d'une session (en secondes)` : indique la durée de validité d'une session SSO sur le serveur. Cela n'influence pas la durée de la session sur les applications authentifiées, seulement la durée de la validité du cookie utilisé par le serveur SSO. Au delà de cette durée, l'utilisateur devra obligatoirement se ré-authentifier pour être reconnu par le serveur SSO. Par défaut, la durée de la session est de 3 heures (7200 secondes).

`CSS par défaut du service SSO (sans le .css)` : permet de spécifier une CSS différente pour le formulaire d'authentification affiché par le serveur EoleSSO. Le fichier CSS doit se trouver dans le répertoire `/usr/share/sso/interface/theme/style/<nom_fichier>.css`. *Se reporter au chapitre personnalisation pour plus de possibilités à ce sujet.*

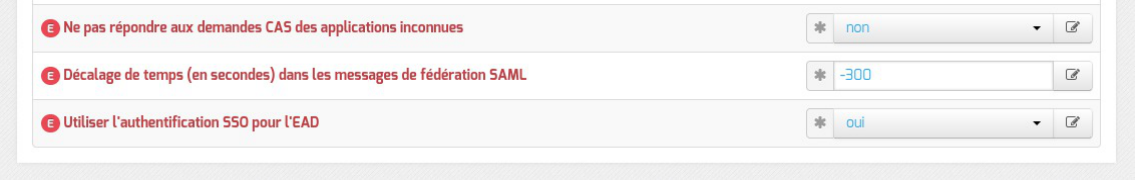
Configuration en mode expert

Options générales

En mode expert 4 nouvelles variables sont disponibles :



- `Activer la balise meta viewport (CSS responsive)` permet d'inclure la balise meta `viewport` dans les pages de l'application (avec content="width=device-width, initial-scale=1"). Elle est à activer en cas d'utilisation d'une feuille de style CSS responsive.



- `Ne pas répondre aux demandes CAS des applications inconnues` est à `non` par défaut

  Si ce paramètre est à oui, seules les applications renseignées dans les fichiers d'applications (`/usr/share/sso/app_filters/*_apps.ini`) sont autorisées à recevoir des réponses du serveur en mode CAS. Si il est à non, le filtre par défaut leur sera appliqué ;

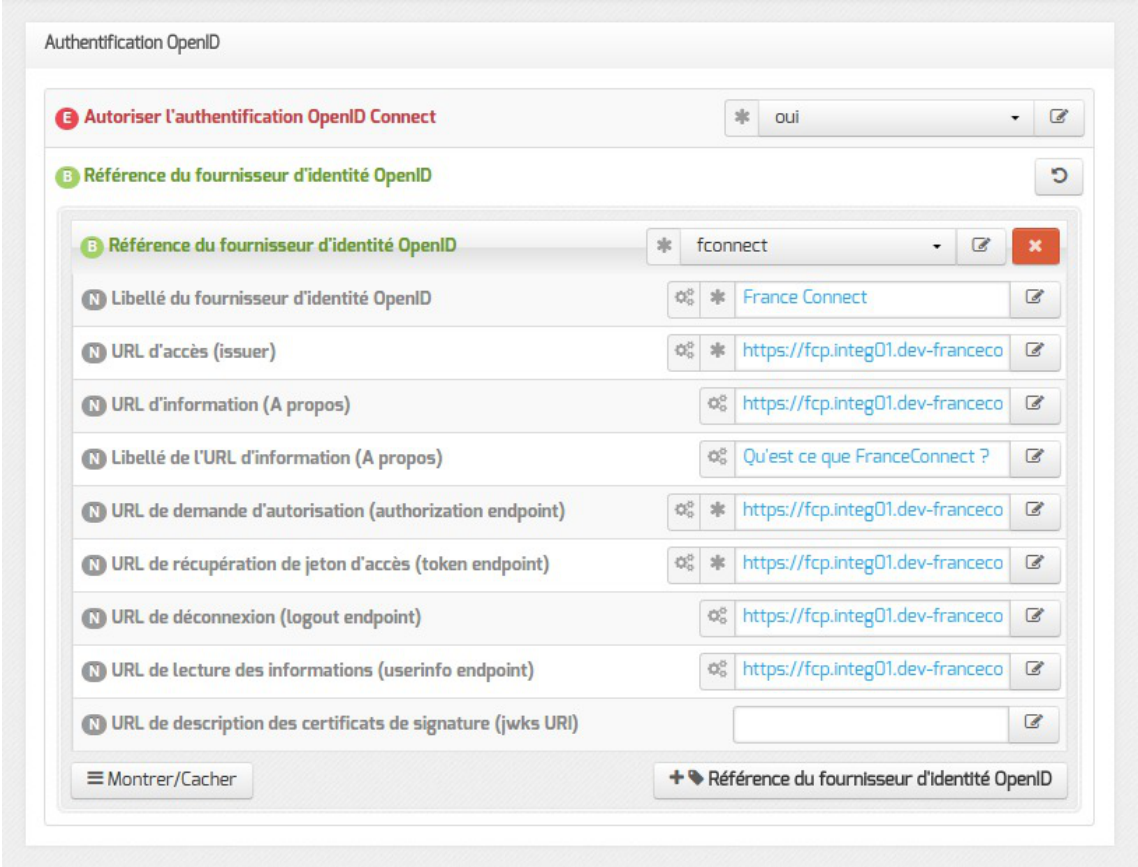
- `Décalage de temps (en secondes) dans les messages de fédération SAML` est à

`-300` secondes par défaut

Ce décalage est appliqué aux dates dans les messages de fédération SAML. Cela permet d'éviter le rejet des messages lorsque le serveur partenaire n'est pas tout à fait synchrone (par défaut, on décale de 5 minutes dans le passé). Ce délai est aussi pris en compte pour la validation des messages reçus ;

- `Utiliser l'authentification SSO pour l'EAD` est à `oui` par défaut. Le passer à `non` permet de ne plus utiliser le serveur SSO pour l'authentification de l'EAD.

Configuration d'authentification OpenID Connect



- `Autoriser l'authentification OpenID Connect` est à `non` par défaut

  Si ce paramètre est à `oui`, il devient possible de configurer un ou plusieurs fournisseurs d'identité OpenID Connect ;
- `Référence du fournisseur d'identité OpenID` : renseigner un libellé pour identifier le fournisseur. Ce libellé est interne à l'application EoleSSO. Il est utilisé pour définir le nom des fichiers contenant les logos/boutons du fournisseur :
  - `/usr/share/sso/interface/images/<libelle>.png` : bouton de connexion présenté sur la page de login (par exemple : "se connecter avec France Connect") ;
  - `/usr/share/sso/interface/images/logo-<libelle>.png` : logo du fournisseur qui sera affiché sur la page d'association de comptes.
- `Libellé du fournisseur d'identité OpenID` : libellé à destination des utilisateurs pour décrire le fournisseur ("France Connect", "Google", ...) ;
- `URL d'accès (issuer)` : URL décrivant le fournisseur d'identité (la plupart du temps, l'URL de

base de son service d'authentification) ;

- `URL de demande d'autorisation (authorization endpoint)` : URL permettant au client d'initier le processus d'authentification ;
- `URL de récupération de jeton d'accès (token endpoint)` : URL permettant de récupérer un jeton (éventuellement l'identifiant de l'utilisateur) après authentification ;
- `URL de déconnexion (logout endpoint)` : URL permettant de demander une déconnexion. Ce paramètre est ignoré pour les fournisseurs utilisant une cinématique de déconnexion spécifique comme Google, Facebook et Microsoft ;
- `URL de lecture des informations (userinfo endpoint)` : URL permettant de récupérer les informations de l'utilisateur à l'aide du jeton fourni ;
- `URL de description des certificats de signature (jwks URI)` : URL décrivant les certificats utilisés par le fournisseur (si disponible) ;

Définition de l'identifiant client (Client ID) et clé secrète (Client secret)

L'identifiant client (Client ID) et la clé privée secrète (Client secret) renvoyés par le fournisseur d'identité utilisés pour valider les échanges doivent être, pour des raisons de sécurité, stockés dans un fichier à part avec des droits restreints.

Pour chaque fournisseur d'identité, ajouter une ligne dans le fichier `/etc/eole/eolesso_openid.conf` :

```
<nom_fournisseur> = "<client id> :<client secret>"
```

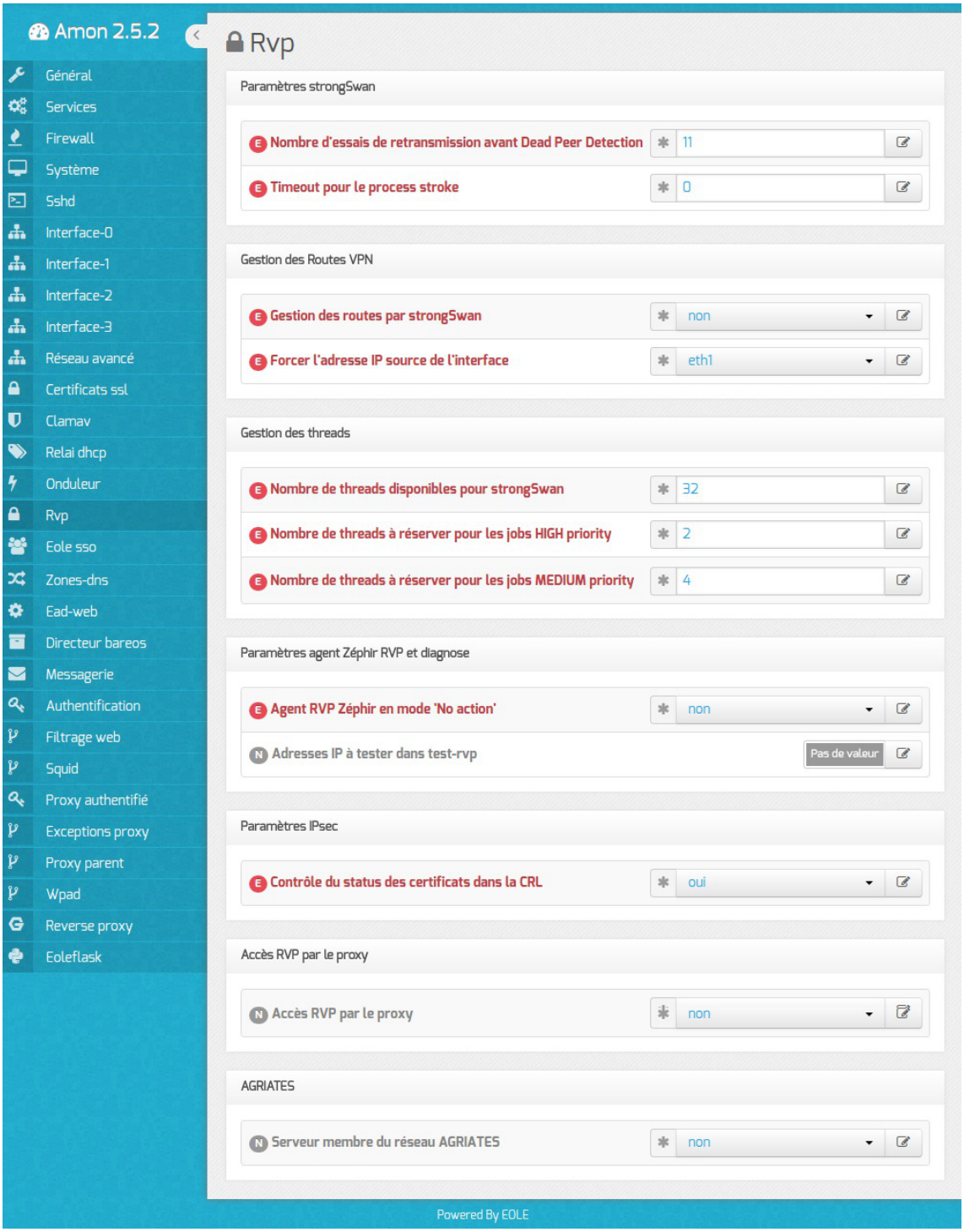
Le `nom_fournisseur` doit correspondre au paramètre `Référence du fournisseur d'identité OpenID` renseigné dans l'interface de configuration du module.

Si ces informations ne sont pas renseignées pour l'un des fournisseurs déclarés, un message l'indiquera au lancement de la commande `diagnose` .

Voir aussi...

- Gestion des sources d'authentification multiples
- Compatibilité OpenID Connnect

3.17. Onglet Rvp : Mettre en place le réseau virtuel privé

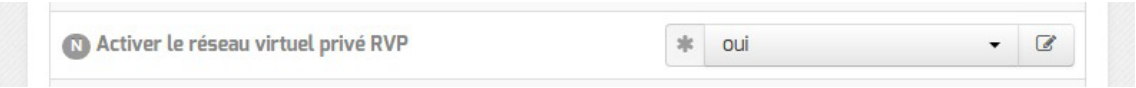


Onglet Rvp mode Expert

Le réseau virtuel privé[p.312] (RVP) peut être activé au moment de la configuration et de l'instanciation d'un module Amon ou sur des modules Amon déjà en exploitation.

Mise en place du RVP

L'onglet `Rvp` apparaît après activation du service dans l'onglet `Services`.



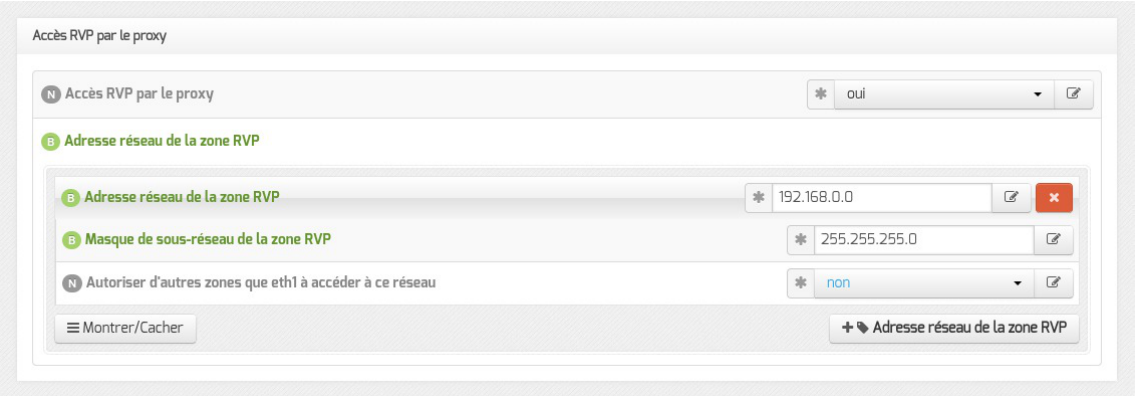
Configuration des tunnels

Le mode VPN database n'est plus supporté et n'est plus disponible à partir de la version 2.5.1 du module Amon. La configuration des tunnels s'effectue d'office en mode fichier plat.

À l'occasion de la mise en place d'un nouveau tunnel avec un serveur Sphynx inférieur à la version EOLE 2.5, il faudra impérativement configurer ce serveur Sphynx en mode database à non.

Accès RVP par le proxy

Pour paramétrer l'accès RVP par le proxy, il faut passer la variable `Accès RVP par le proxy` à `oui`.



L'adresse réseau de la zone RVP permet la configuration du proxy Squid pour autoriser ou non, aux postes autres que sur l'interface eth1, l'accès via le VPN à un sous réseau.

Pour ajouter d'autres adresses réseau il faut cliquer sur le bouton `+Adresse réseau de la zone RVP`.

Paramètres agent Zéphir RVP et diagnose

Le champ `Adresses IP à tester dans test-rvp` permet de saisir une ou plusieurs adresses IP qui seront utilisées par le diagnose et par l'agent Zéphir pour tester des adresses IP à l'autre extrémité des tunnels.

AGRIATES

Si le serveur est membre d'AGRIATES il faut passer la variable `Serveur membre du réseau AGRIATES` à `oui`.

- `Adresse du DNS permettant de résoudre les in.ac-acad.fr` permet de spécifier l'adresse IP du serveur DNS permettant de résoudre les noms de zone AGRIATES (in.ac-académie.fr) ;
- `Nom DNS de la zone résolue par le DNS AGRIATES` : permet de spécifier d'autres noms de zones résolues par le DNS AGRIATES.

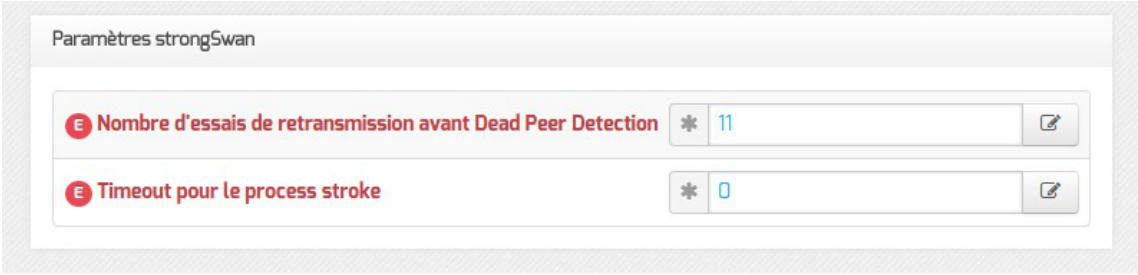
Paramètres propres au mode expert

Le mode Expert permet de personnaliser le fonctionnement de strongSwan.

`Forcer l'encapsulation (Détection NAT)`, si la valeur est à `oui`, cela force la socket UDP/4500 pour l'établissement des connexions. Si la valeur est à `non`, le socket est fixé à UDP/500 sauf s'il y a détection de NAT (UDP/4500).

`Autoriser le changement d'adresse IP d'une extrémité de connexion` (MOBIKE IKEv2 extension - RFC 4555) permet à une extrémité de changer d'adresse IP pour une connexion donnée. Dans ce cas, la connexion se fera toujours sur UDP/4500.

Paramètres strongSwan



Onglet Rvp mode Expert

`Nombre d'essais de retransmission avant Dead Peer Detection` indique à strongSwan le nombre d'essais de reconnexion avant l'abandon.

`Timeout pour le process stroke` permet de fixer le nombre de millisecondes avant l'arrêt forcé de processus qui se seraient figés.

> La variable `Configuration des tunnels en mode database` n'est plus disponible dans la version 2.5 d'EOLE, ce mode a été supprimé au profit du mode fichier plat.

Gestion des Routes VPN

Onglet Rvp mode Expert

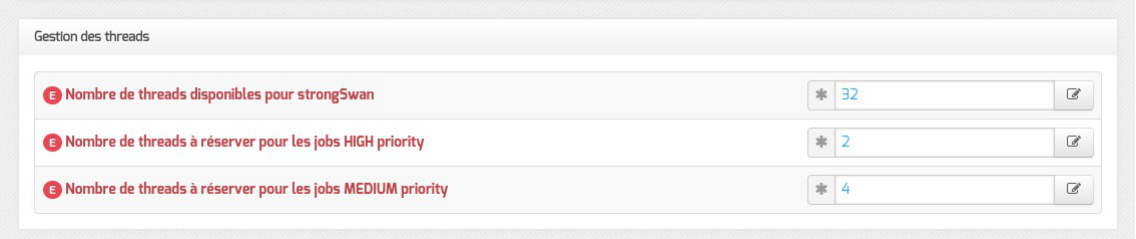
`Gestion des routes par strongSwan` permet si la valeur est passée à `non` de faire gérer la mise en place des routes concernant les tunnels par un script.

Exemple, dans notre cas et sur le module Amon uniquement :

`/etc/ipsec.d/ipsec_updown`

`Forcer l'adresse IP source de l'interface` permet de forcer l'adresse IP que le serveur utilisera pour entrer dans les tunnels. Cette option est utilisée sur les serveur Amon afin d'éviter qu'ils utilisent aléatoirement l'adresse IP de l'une de ses interfaces lorsqu'ils passent dans un tunnel.

Gestion des threads



Onglet Rvp mode Expert

`Nombre de threads disponibles pour strongSwan` permet d'allouer un nombre de fils d'exécution maximum pour ses différentes tâches. Une valeur trop petite peut entraîner des mises en file d'attente importantes.

`Nombre de threads à réserver pour les jobs HIGH priority` réserve une nombre de fils d'exécution minimum pour les tâches HIGH priority (`ipsec stroke` et DPD). La valeur `1` ou `2` maximum est idéale.

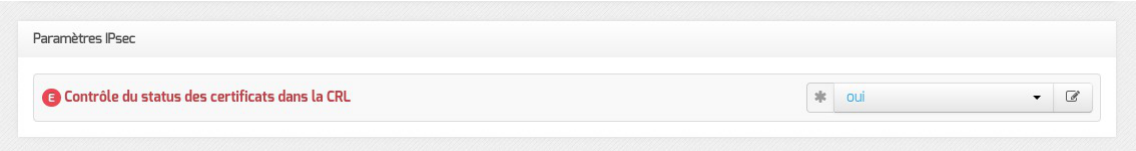
`Nombre de threads à réserver pour les jobs MEDIUM priority` réserve une nombre de fils d'exécution minimum pour les tâches MEDIUM priority (Initialisation de connexion entre autres).

Paramètres agent Zéphir RVP et diagnose

Onglet Rvp mode Expert

`Agent rvp Zéphir en mode 'No action'` permet de paramétrer l'agent RVP pour ne rien faire en cas de détection de tunnels défectueux (pas de coupure/relance des tunnels).

Paramètres IPsec



Onglet Rvp mode Expert

Active ou non la vérification de la validité d'un certificat dans la liste de révocation (CRL[p.303]).

Application de la configuration et gestion du RVP

Activation du RVP au moment de l'instanciation du serveur Amon

Au lancement de l'instanciation, la question suivante vous est posée :

`Voulez-vous configurer le Réseau Virtuel Privé maintenant ? [oui/non] [non] :`

Vous devez répondre `oui` à cette question.

Deux choix sont alors proposés :

`1.Manuel` permet de prendre en compte la configuration RVP présente sur une clé USB ;

`2.Zéphir` active la configuration RVP présente sur le serveur Zéphir. Cela suppose que le serveur est déjà enregistré sur Zéphir. Il sera demandé un compte Zéphir et son code secret ainsi que l'identifiant Zéphir du serveur Sphynx auquel associer le module Amon.

Dans les deux cas, le code secret de la clé privée est demandée. Si le code secret est correct le RVP est configuré pour cette machine et l'instanciation peut se poursuivre...

Activation du RVP sur des modules Amon déjà en exploitation

Pour activer un RVP sur un module Amon déjà instancié, il faut lancer en tant qu'utilisateur `root` la commande `active_rvp init`.

Suppression du RVP

Pour supprimer un RVP, il faut lancer en tant qu'utilisateur `root` la commande `active_rvp delete`.

3.18. Onglet Zones-dns : Configuration du DNS

EOLE propose un serveur DNS[p.304] local qui a pour rôles principaux de servir de cache afin d'accélérer les requêtes et de résoudre certains noms de domaines locaux.

Dans le cadre du module Amon, il est en mesure de gérer les différentes zones du réseau établissement.

La génération des différents fichiers de configuration (fichiers de zones) est effectuée par un programme appelé `h2n`.

Il est possible, depuis l'interface de configuration du module, d'activer ou non certaines fonctionnalités et d'ajouter des valeurs au niveau du DNS.

Configuration DNS sur l'interface-0

Sur une installation en mode une carte (exemple : EoleBase + `eole-dns`), le DNS est activable ou désactivable dans l'onglet `Interface-0` avec la variable : `Activer le serveur DNS sur cette zone`.

Configuration du DNS sur eth0

Sur le module Amon et ses variantes (AmonEcole, AmonEcole+), cette question est également présente dans l'onglet `Interface-0`.

Pour chacune des interfaces configurées, il est possible de préciser si le DNS est maître de la zone en passant la variable `Serveur master DNS sur cette zone` à `oui`.

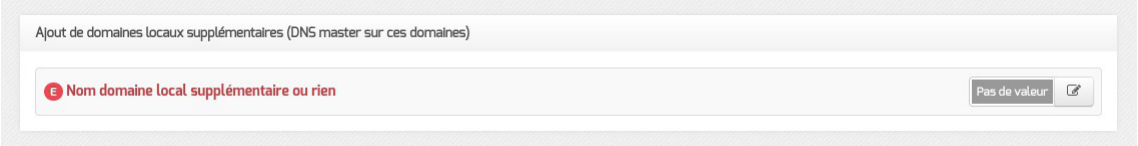
Au moins une des zones doit être configurée en maître de la zone.

Personnalisation des zones DNS

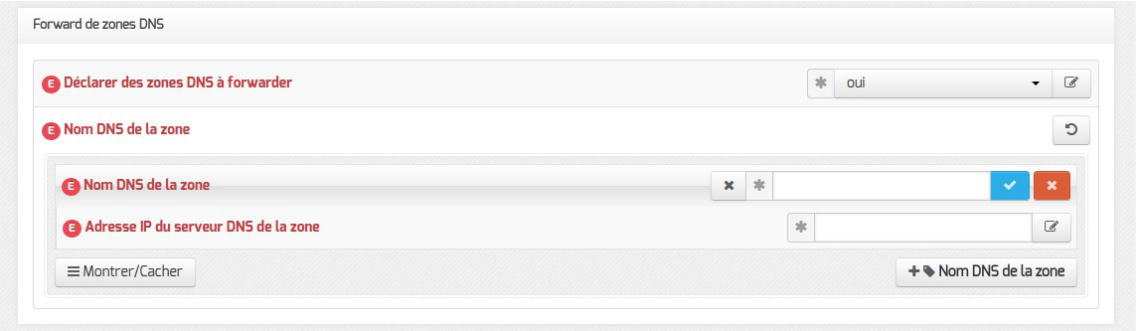
L'onglet expert `Zones-dns` comporte plusieurs variables directement liées au DNS.

L'onglet Zones-dns

Le champs `Nom de domaine local supplémentaire ou rien` permet au serveur DNS de résoudre les noms de ce domaine.



Si un nom d'hôte avec un suffixe DNS différent du nom de domaine privé du réseau local est déclaré, il est nécessaire de renseigner ce suffixe ici pour que le serveur DNS puisse résoudre ce nom.



Certaines zones nécessitent l'utilisation d'un serveur DNS particulier.

En passant la variable `Déclarer des zones DNS à forwarder` à `oui`, il est possible de saisir le nom d'une zone et l'adresse IP de son DNS de forward dans les champs `Nom DNS de la zone` et `Adresse IP du serveur DNS de la zone`.

La déclaration de serveurs locaux (`Ajouts d'hôtes dans le DNS`) ne se fait plus dans l'onglet `Zones-dns` mais dans l'onglet `Réseau avancé`.

DNS et RVP

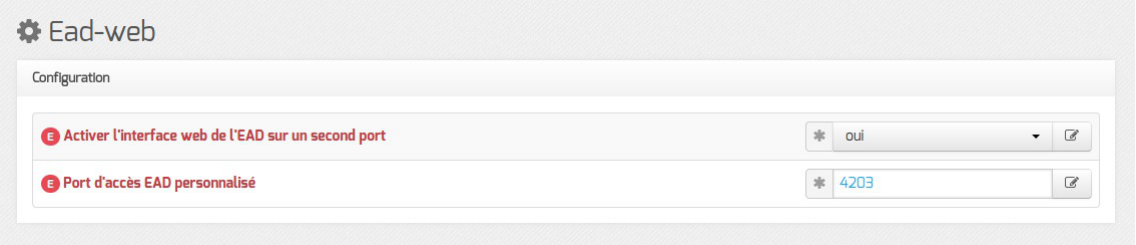
Si le réseau privé virtuel (RVP[p.312]) est activé et configuré sur le serveur et que le serveur est membre du réseau privé de l'Éducation nationale (AGRIATES[p.301]), il devient possible de déclarer, dans l'onglet `Rvp`, le DNS interne à utiliser pour résoudre les noms de domaines.

L'onglet Rvp

Il est possible de renseigner un ou plusieurs serveurs DNS AGRIATES dans le champs `Adresse du DNS permettant de resoudre les in.ac-acad.fr`. Des relais de zones "AGRIATES" sont prédéfinis et correspondent aux zones *in* du domaine académique. D'autres relais de zone pour le DNS AGRIATES peuvent être ajoutés dans le champs `Nom DNS de la zone resolue par le DNS AGRIATES`.

3.19. Onglet Ead-web : EAD et proxy inverse

Si l'interface web de l'EAD est activée sur le module (onglet `Services`), les paramètres de l'onglet `Ead-web` permettent de régler le port d'accès à l'interface EAD depuis l'extérieur si un proxy inverse est utilisé.



Par défaut l'utilisation d'un proxy inverse pour accéder à l'EAD est à `non`.

Si la variable est passée à `oui`, le port proposé pour accéder à l'EAD depuis l'extérieur est par défaut 4203.

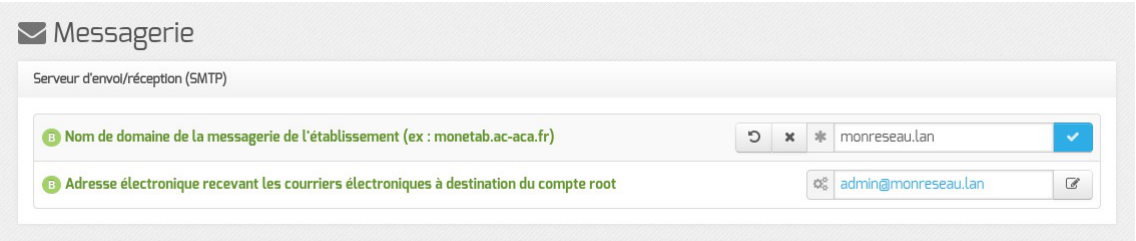
3.20. Onglet Messagerie

Même sur les modules ne fournissant aucun service directement lié à la messagerie, il est nécessaire de configurer une passerelle SMTP valide car de nombreux outils sont susceptibles de nécessiter l'envoi de mails.

La plupart des besoins concernent l'envoi d'alertes ou de rapports.

Exemples : rapports de sauvegarde, alertes système, ...

Serveur d'envoi/réception



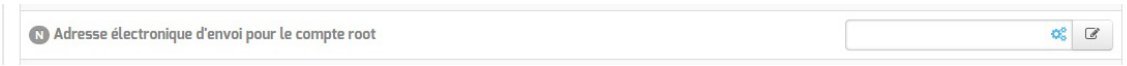
Les paramètres communs à renseigner sont les suivants :

- `Nom de domaine de la messagerie de l'établissement (ex : monetab.ac-aca.fr)`, saisir un nom de domaine valide, par défaut un domaine privé est automatiquement créé avec le préfixe `i-`;
- `Adresse électronique recevant les courriers électroniques à destination du compte root`, permet de configurer une adresse pour recevoir les éventuels messages envoyés par le système.

Le `Nom de domaine de la messagerie de l'établissement` (onglet `Messagerie`) ne peut pas être le même que celui d'un conteneur. Le nom de la machine (onglet `Général`) donne son nom au conteneur maître aussi le `Nom de domaine de la messagerie de l'établissement` ne peut pas avoir la même valeur.

Dans le cas contraire les courriers électroniques utilisant le nom de domaine de la messagerie de l'établissement seront réécris et envoyés à l'adresse électronique d'envoi du compte root.

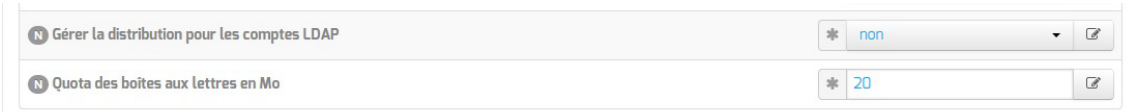
> Cette contrainte permet de faire en sorte que les courrier électroniques utilisant un domaine de type `@<NOM_CONTENEUR>.*` soit considéré comme des courriers électroniques systèmes.



En mode normal il est possible de configurer le nom de l'émetteur des messages pour le compte `root`.

> Certaines passerelles n'acceptent que des adresses de leur domaine.

Toujours en mode normal d'autres paramètres sont modifiables.



Passer `Gérer la distribution pour les comptes LDAP` à `oui` active les transports LDAP pour la distribution des courriers électroniques, la distribution des courriers locaux est forcée ainsi ils ne sont pas mis en queue et supprimés une semaine plus tard.

Il est également possible de changer la taille des quotas de boîtes aux lettres électroniques qui est fixé par défaut à 20 Mo.

En mode expert il est possible d'écraser l'entêtes des courriers électroniques.

La réécriture des adresses doit prendre en compte la distinction entre l'enveloppe SMTP (« MAIL FROM » et « RCPT TO ») et les en-têtes des messages (« From: », « Reply-To:», « To: », « Cc: », « Bcc: »).

Les adresses électroniques systèmes ont par défaut une des formes suivante :

- `user@%%domaine_messagerie_etab` si l'expéditeur ne précise pas le nom de domaine, par exemple :

  ```
  root@internet:~# echo "Test" | mail -s "Test mail from shell" -r root root
  ```

- `user@%%nom_machine.%%domaine_messagerie_etab` pour le maître si l'expéditeur utilise la configuration définie dans `/etc/mailname`
- `user@%%conteneur.%%nom_machine.%%domaine_messagerie_etab` pour les conteneurs[p. 303] si l'expéditeur utilise la configuration définie dans `/etc/mailname`

Si la valeur de `%%nom_domaine_local` est différente de la valeur de `%%domaine_messagerie_etab`, alors on force les formes suivantes pour le maître et les conteneurs uniquement :

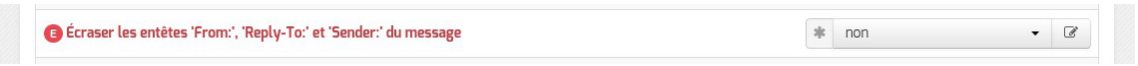
- `user@%%nom_machine.%%domaine_messagerie_etab` pour le maître
- `user@%%conteneur.%%nom_machine.%%domaine_messagerie_etab` pour les conteneurs

Les adresses destinataires `root@%%nom_domaine_local` et `root@%%domaine_messagerie_etab` sont remplacées par `%%system_mail_to` si cette dernière

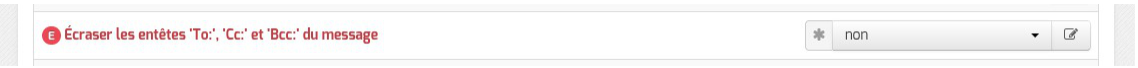
est définie.

Les adresses expéditeurs et destinataires systèmes sont ensuite réécrites selon les tableaux suivants en fonction de variables expertes :

- `system mail from for headers` : écraser les en-têtes « From: », « Reply-To: » et « Sender: » du message, par défaut à `non`



- `system mail to for headers` : écraser les en-têtes « To: », « Cc: » et « Bcc: » du message, par défaut à `non`



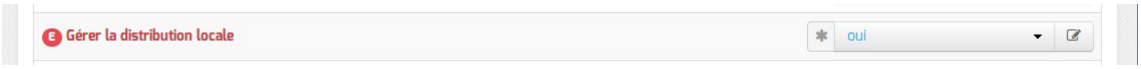
Réécriture de l'expéditeur :

	system_mail_from_for_headers = non	system_mail_from_for_headers = oui
MAIL FROM	system_mail_from	system_mail_from
From :	user@conteneur.machine.domaine	system_mail_from
Reply-To :	user@conteneur.machine.domaine	system_mail_from
Sender :	user@conteneur.machine.domaine	system_mail_from

Réécriture du destinataire :

	system_mail_to_for_headers = non	system_mail_to_for_headers = oui
RCPT TO	system_mail_to	system_mail_to
To :	user@conteneur.machine.domaine	system_mail_to
Cc :	user@conteneur.machine.domaine	system_mail_to
Bcc :	user@conteneur.machine.domaine	system_mail_to

Par défaut la distribution des messages se fait en local, ce qui permet d'avoir un domaine local et un domaine privé.

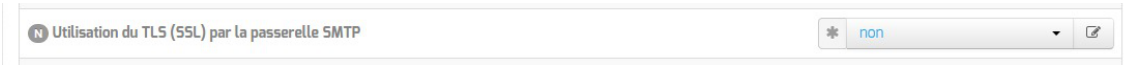


Dans ce cas il est possible d'agir sur le quota des boîtes et sur le pourcentage d'occupation, qui entraîne un message électronique d'avertissement.

Relai des messages

La variable `Passerelle SMTP`, permet de saisir l'adresse IP ou le nom DNS de la passerelle SMTP à utiliser.

> Afin d'envoyer directement des courriers électroniques sur Internet il est possible de désactiver l'utilisation d'une passerelle en passant `Router les courriels par une passerelle SMTP` à `non`.
>
> Sur les modules possédant un serveur SMTP (Scribe, AmonEcole), ces paramètres sont légèrement différents et des services supplémentaires sont configurables.



`Utilisation du TLS (SSL) par la passerelle SMTP` permet d'activer le support du TLS[p.314] pour l'envoi de message. Si la passerelle SMTP[p.313] accepte le TLS, il faut choisir le port en fonction du support de la commande STARTTLS[p.313] (port 25) ou non (port 465).

Par défaut le relai des messages n'est pas activé sur les modules sauf sur le module Seshat. Si la variable est passée à oui, elle active les listes d'adresses IP autorisées à utiliser ce serveur comme relai de messagerie et la liste des noms de domaines autorisés à être relayés par ce serveur.

Le TLS est activé par défaut pour les clients.

Dans la rubrique Configuration experte plusieurs paramètres peuvent être modifiés.

- `FQDN utilisé par Exim`
  Personnalisation du nom de domaine complètement qualifié utilisé par Exim dans le protocole SMTP.

C'est utile pour les vérifications anti-spam des MX externes

Les valeurs possibles sont :

- automatique : laisser Exim décider ;
- nom_machine.domaine_messagerie_etab : utiliser le nom de la machine complété par le nom de domaine de la messagerie établissement ;
- nom_machine.nom_domaine_local : utiliser le nom de la machine complété par le nom de domaine local.

- `Domaine utilisé pour qualifier les adresses`

  Nom de domaine ajouté aux adresses :

  - nom de domaine local ;
  - domaine privé de messagerie établissement ;
  - domaine public de messagerie établissement.

- `Envoyer les logs à rsyslog`

  Permet de désactiver l'envoi des logs.

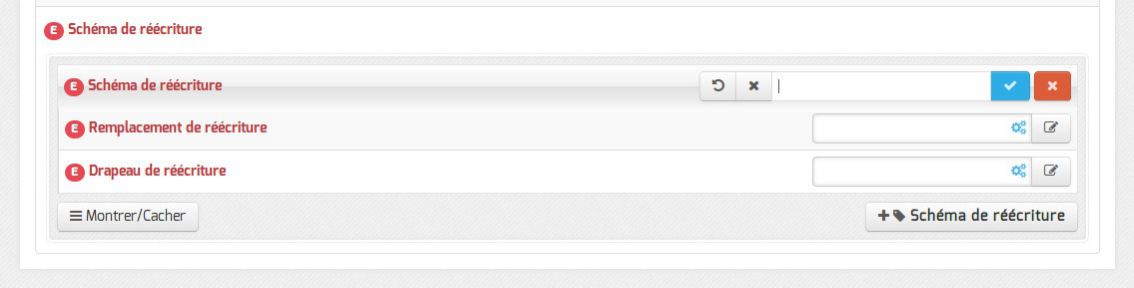
- `Dupliquer les logs dans des fichiers`

  Dupliquer les logs dans des fichiers gérés directement par Exim. Si vous envoyez les logs à syslog, vous pouvez conserver la gestion des fichiers traditionnelle d'Exim. Ces fichiers étant gérés directement par Exim, ils se trouveront dans le conteneur du service.

- `Activer les règles de réécriture étendue`

  Permettre de définir des règles de réécriture personnalisées. Si non, seuls les courriers électroniques en `localhost` sont réécrits avec le `nom domain local`.

  http://exim.org/exim-html-current/doc/html/spec_html/ch31.html.



Les trois variables à saisir sont :

- Modèle de correspondance des adresses courriers électroniques à réécrire : http://exim.org/exim-html-current/doc/html/spec_html/ch31.html#SECID151
- Valeur de remplacement des adresses électroniques : http://exim.org/exim-html-current/doc/html/spec_html/ch31.html#SECID152
- Drapeau contrôlant la réécriture des adresses électroniques : http://exim.org/exim-html-current/doc/html/spec_html/ch31.html#SECID153

3.21. Onglet Authentification : Configuration du proxy authentifié et de FreeRADIUS

EOLE propose un mécanisme d'authentification web via un proxy.

Tous les accès web (HTTP et HTTPS) nécessiteront alors une phase d'authentification.

Cette fonctionnalité offre deux avantages :

- il sera possible de savoir quel utilisateur a accédé à une ressource particulière ;
- il sera possible d'appliquer des politiques de filtrage pour chaque utilisateur.

Pour profiter de cette fonctionnalité, il faut activer l'authentification du proxy dans l'onglet `Authentification` : `Activer l'authentification web (proxy)`.

Cinq méthodes d'authentification sont alors disponibles dans l'onglet `Proxy authentifié`.

Activer une deuxième instance de Squid

Activer une deuxième instance de Squid permet une double authentification, c'est à dire la possibilité de pouvoir configurer deux types distincts d'authentification proxy.

Par exemple, pouvoir utiliser à la fois une authentification NTLM/SMB et une authentification LDAP.

L'implémentation retenue est d'utiliser une instance du logiciel Squid par type d'authentification.

Pour profiter de cette fonctionnalité, il faut passer `Activer une deuxième instance de Squid` à `oui`.

Cela fera apparaître l'onglet `Proxy authentifié 2`.

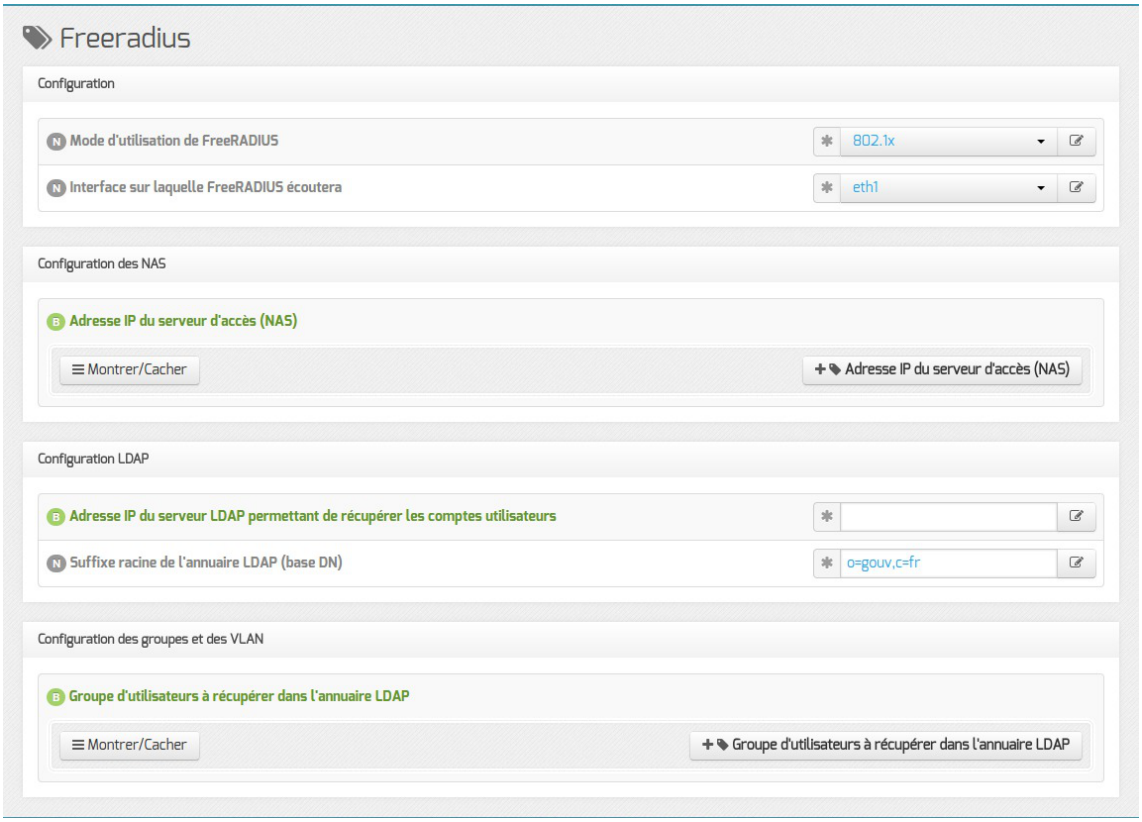
En mode expert cela fera apparaître également l'onglet `Squid2`.

Activer le service FreeRADIUS

EOLE propose un mécanisme d'authentification réseau basée sur le protocole RADIUS[p.312].

Pour profiter de cette fonctionnalité, il faut activer le service d'authentification RADIUS en passant `Activer le service FreeRADIUS` à `oui`.

Cela fera apparaître l'onglet `Freeradius`.



Vue de l'onglet Freeradius de l'interface de configuration du module

Voir aussi...

Onglet Proxy authentifié : 5 méthodes d'authentification [p.74]

Onglets Squid2 et Proxy authentifié 2 : Double authentification [p.171]

Onglet Freeradius : Configuration de l'authentification Radius [p.85]

3.22. Onglet Filtrage web : Configuration du filtrage web

EOLE permet de différencier les zones suivant l'interface (administration ou pédagogie).

La différenciation se fait en modifiant la valeur choisie pour `Filtre Web à appliquer à cette interface` dans la configuration de l'interface (onglets : `Interface-1`, `Interface-2`, ...).

Les filtres web 1 et 2 correspondent chacun à une instance du logiciel de filtrage.

Le module Amon intègre le logiciel libre e2guardian[p.304] pour réaliser le filtrage web.

Le paramétrage par défaut de e2guardian convient à un établissement de taille moyenne sans modification particulière.

Il peut être néanmoins intéressant de modifier ce paramétrage pour satisfaire les besoins de l'établissement (notamment dans le cas où le serveur ne peut plus répondre aux requêtes, la fenêtre

d'authentification apparaît de façon intempestive, ...).

Sur un petit établissement, il sera possible d'économiser des ressources.

Sur un gros établissement, il pourra répondre à un plus grand nombre de requêtes.

Un certain nombre de paramétrages sont proposés pour contrôler les ressources de e2guardian.

Il est possible d'affecter une politique spécifique aux machines du foyer (politique plus laxiste) et une autre aux machines du CDI (politique moins permissive).

Politiques de filtrage optionnelles

Une politique de filtrage correspond à un ensemble d'autorisations ou interdictions d'accès à des sites, suivant différents critères.

Il existe par défaut 4 politiques obligatoires :

- une politique de filtrage par défaut ;
- une politique « modérateur » (permet d'outrepasser les interdictions) ;
- une politique « interdits » (permet d'interdire toute navigation) ;
- une politique « liste blanche » (navigation limitée aux sites de cette même liste).

Seule la politique de filtrage par défaut est modifiable via l'EAD.

En plus de ces politiques, il est possible d'ajouter de 1 à 4 autres politiques de filtrage optionnelles (il y en a 3 par défaut).

Ces politiques de filtrage optionnelles seront alors paramétrables dans l'EAD.

Pour modifier le nombre de politiques de filtrage par zone, il faut utiliser le paramètre :

`Nombre de politiques optionnelles de filtrage par zone`.

La valeur 0 revient à n'utiliser que les 4 politiques par défaut proposées ci-dessus.

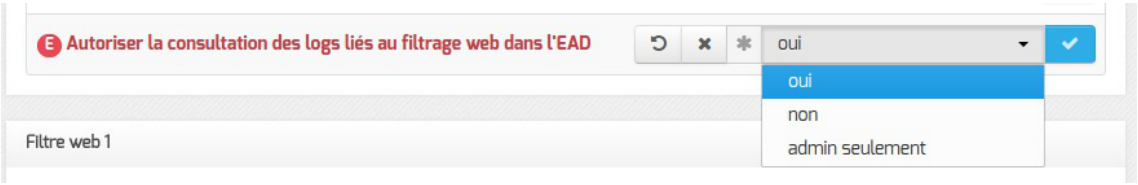
L'ajout de politiques optionnelles (valeur 1,2,3,4) permet d'ajouter des filtres supplémentaires, associables à des groupes de machines ou des comptes utilisateur.

Plus vous définissez de politiques, plus e2guardian utilisera de ressources.

Adaptez le nombre de politiques activées en fonction de vos besoins.

L'observatoire des navigations

L'observatoire des navigations est un outil de consultation des logs de l'outil de filtrage e2guardian[p.304].



La question `Autoriser la consultation des logs liés au filtrage web dans l'EAD` propose plusieurs options :

- `oui` : accès autorisé pour les utilisateurs EAD possédant les actions `navigation_visit_admin` et/ou `navigation_visit_pedago` ;
- `non` : accès interdit pour tout le monde, personne ne voit le lien `Visites des sites` (configuration par défaut) ;
- `admin seulement` : accès autorisé uniquement pour le rôle `admin`.

La consultation des visites de sites se fait au travers de l'EAD, menu : `Filtre web X/visites des sites`.

Paramétrage de e2guardian

Le logiciel e2guardian offre de nombreuses options de configuration.

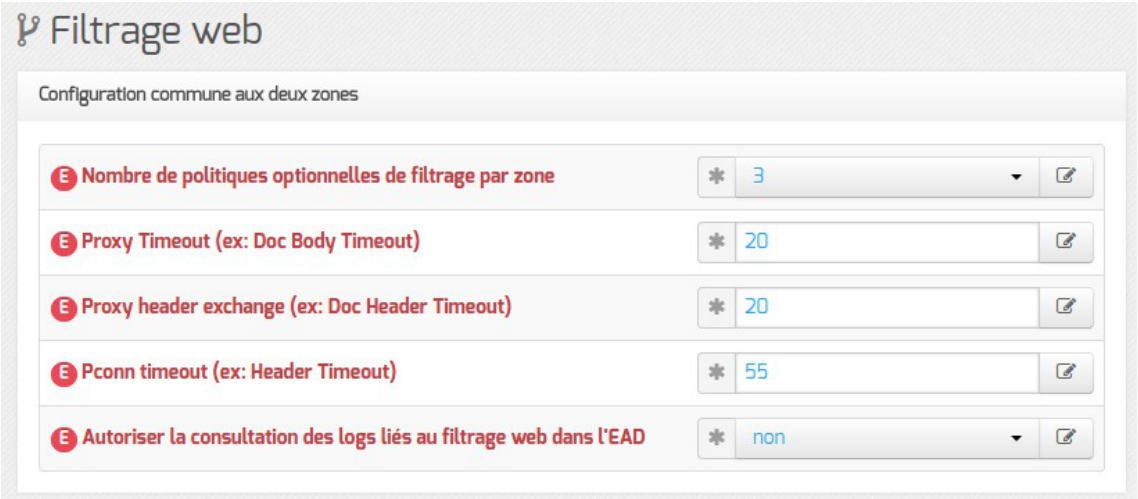
Plusieurs sont paramétrables dans l'interface de configuration du module.

Seule l'expérience «à tâtons»[p.307] permet de définir les valeurs adéquates à votre installation.

L'objectif est d'utiliser le plus de mémoire possible sans que le serveur n'utilise la partition d'échange (swap[p.313]) .

La commande `top` en console permet d'observer l'évolution de l'utilisation de la partition d'échange de façon dynamique.

Les options de configuration proposées dans la première partie de l'interface de configuration sont communes aux deux zones configurables :



Proxy Timeout (ex: Doc Body Timeout)

Délai d'attente TCP entre le proxy et e2guardian (en secondes).

Proxy header exchange (ex: Doc Header Timeout)

Délai d'attente entre le proxy et e2guardian (en secondes).

Pconn timeout (ex: Header Timeout)

Délai pendant lequel une connexion persistante attend de nouvelles requêtes (en secondes).

Les options de configuration proposées dans les sections suivantes permettent de personnaliser la configuration de chacune des zones configurables.

Nombre maximum de processus

Le nombre maximum de processus disponibles pour traiter les nouvelles connexions. La valeur par défaut est fixée à 256, elle peut être modifiée et doit être comprise entre 80 et 8192.

Il est fortement recommandé de ne pas dépasser la valeur maximum de 8192 processus.

Nombre minimum de processus

Le nombre de processus minimal pour traiter les nouvelles connexions.

Nombre minimum de processus en attente

Le nombre minimum de processus prêts à recevoir de nouvelles connexions.

Nombre maximum de processus en attente

Le nombre maximum de processus attendant de nouvelles connexions.

Nombre de processus démarré s'il en manque

Le nombre minimum de processus disponibles lorsqu'ils viennent à manquer.

Durée de vie maximum d'un processus avant de se terminer

Les processus enfant, comme tout processus, peuvent succomber à des variables parasites. Ce paramètre définit l'âge maximal de connexions qu'un processus enfant traite avant de quitter. La valeur par défaut est de traiter 500 demandes de connexion avant de quitter.

Augmenter ce paramètre peut aider à soulager les problèmes de performance liés à la rotation des processus, mais peut créer un problème de performance si un processus s'emballe pour une raison quelconque.

Sur les grands sites vous pourriez vouloir essayer de passer cette valeur à 10000.

Répertoire de cache

Permet de choisir le chemin du répertoire de cache, par défaut `/tmp`.

La taille maximum de fichier conservé en mémoire

Cette variable n'est utilisée que si vous utilisez un greffon d'anti-virus.

C'est la taille maximale des fichiers en kibibytes[p.311] que e2guardian va télécharger et mettre en cache dans la RAM. Après que cette limite soit atteinte, e2guardian met en cache sur le disque.

Cette valeur doit être inférieure ou égale à la valeur de `La taille maximum de fichier conservé sur le disque`.

Utiliser la valeur 0 permet de définir le même réglage que `La taille maximum de fichier conservé sur le disque`.

La taille maximum de fichier conservé sur le disque

Cette variable n'est utilisée que si vous utilisez un greffon d'anti-virus.

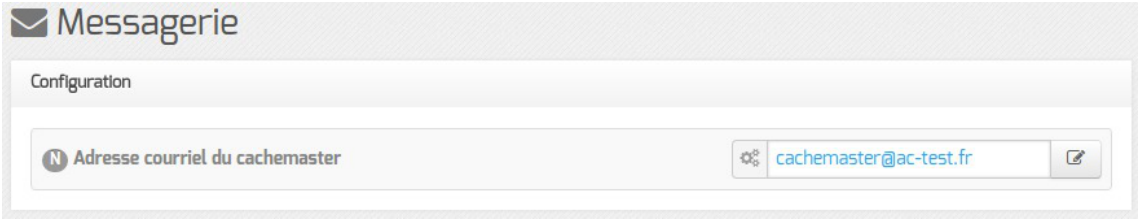
C'est la taille maximale des fichiers en kibibytes[p.311] que e2guardian va télécharger de sorte qu'ils soient vérifiés par l'anti-virus.

Cette valeur doit être supérieure ou égale à `La taille maximum de fichier conservé en mémoire`.

Adresse électronique à utiliser en cas de réclamation

Lorsque la consultation d'une page est refusée à l'utilisateur, une page d'erreur affichant les détails de l'interdiction apparaît.

Celle-ci propose également une adresse électronique à utiliser pour signaler les interdictions injustifiées.



Cette adresse se configure par l'intermédiaire de la variable `Adresse courriel du cachemaster` disponible dans l'onglet `Messagerie`.

Désactivation du filtrage web

Dans certaines configurations (utilisation d'un proxy académique, ...), il peut s'avérer utile de désactiver complétement le filtrage web.

Cela est possible en allant dans l'interface de configuration du module en mode expert et en répondant `non` à la question de l'onglet `Services`, `Activer le filtrage sur le proxy`.

Dans cette configuration, le proxy Squid écoute sur le **port 3128** en lieu et place du logiciel de filtrage e2guardian.

Voir aussi...

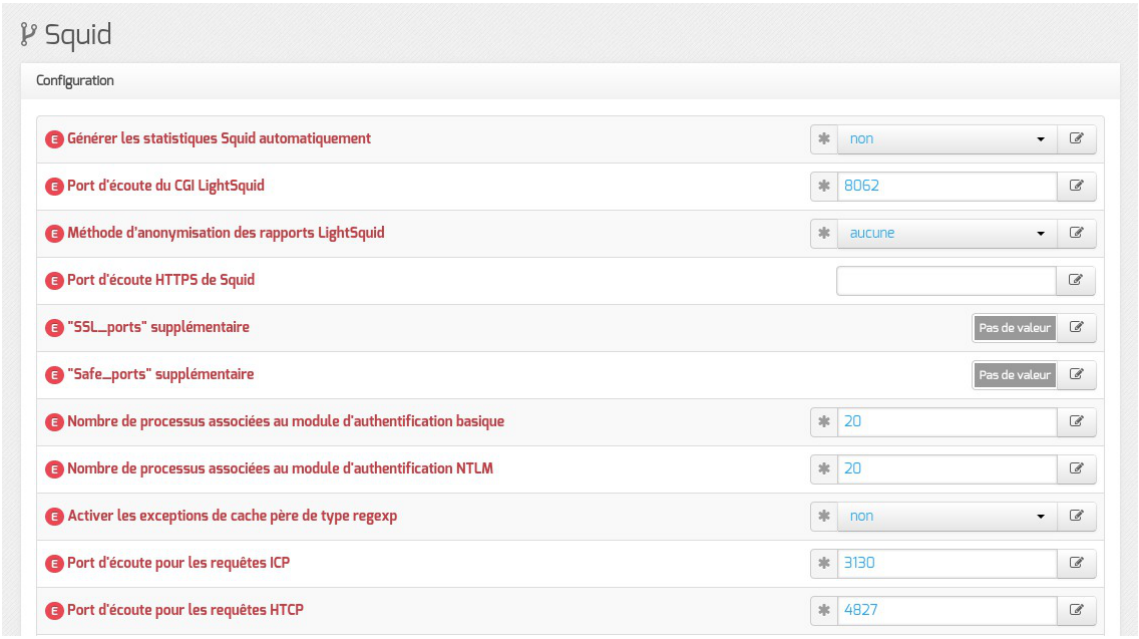
Observatoire des navigations [p.231]

3.23. Onglet Squid : Configuration du proxy

Le service proxy Squid n'étant pas désactivable, l'onglet `Squid` est toujours accessible en mode expert.

L'onglet expert `Squid` permet de modifier et de fixer une sélection des principaux paramètres du fichier de configuration : `/etc/squid3/squid.conf`.

Les paramètres de ce fichier de configuration se retrouvent explicitement dans le nom des variables Creole (mode Debug de l'interface de configuration du module).



Vue de l'onglet Squid de l'interface de configuration du module

Paramétrer l'analyse de logs LightSquid

Les options `Générer les statistiques Squid automatiquement`, `Port d'écoute du CGI LightSquid` et `Méthode d'anonymisation des rapports LightSquid` servent à

configurer l'outil d'analyse de logs LightSquid permettant d'afficher sous forme de pages web l'utilisation du proxy. Sa configuration fait l'objet d'une section dédiée.

Paramétrer les ports d'écoute de Squid

L'option `Port d'écoute HTTP de Squid` est par défaut fixée au port `8080` et n'est à modifier que si le filtrage web a été désactivé.

Il est possible de paramétrer Squid pour qu'il écoute les requêtes HTTPS des clients. Ceci est particulièrement utile dans les situations où vous utilisez Squid comme accélérateur des requêtes.

Il faut alors saisir le numéro de port choisi dans le champ `Port d'écoute HTTPS de Squid`.

Par défaut, un certain nombre de ports SSL sont paramétrés et considérés comme sûrs quand ils sont des ports sortants : 443, 563, 631, 4000-5000, 8070, 8090, 8443, 8753 et 7070. Il est possible d'en ajouter autant que vous voulez dans le champ `"SSL ports" supplémentaire`.

Par défaut, un certain nombre de ports sont définis et autorisés aux utilisateurs : 80, 21, 443, 563, 70, 210, 631 et 1025-65535. Il est possible d'en ajouter autant que vous voulez dans le champ `"Safe ports" supplémentaire`.

Personnaliser la durée des caches

L'option `Personnaliser sélectivement la durée des caches`, présente à partir de la version 2.5.2 d'EOLE, permet de personnaliser l'algorithme de gestion du rafraîchissement du cache par site.

La gestion du cache de Squid peut ne pas correspondre à tous les sites. Par exemple, pour les sites antiviraux, il vaut mieux augmenter la durée de conservation du cache des fichiers téléchargés par les postes clients.

Voici un exemple la configuration à mettre en place pour conserver en cache les signatures de l'anti-virus Trend :

L'expression rationnelle décrit la chaîne de caractères et les règles qui permettent de construire l'URL :

- **^** marque le début d'une chaîne ;
- **$** marque la fin d'une chaîne ;

- | marque l'alternative ;
- . indique n'importe quel caractère ;
- * aucune, une ou plusieurs occurrences du caractère.

Les variables qui permettent de régler le comportement du cache de Squid sont :

- `Temps maximum de cache` ;
- `Rapport entre l'âge de l'objet dans le cache et son âge sur le site` ;
- `Temps minimum de cache`.

Cette configuration générera la ligne de configuration suivante :

- `refresh pattern -i <url regexp> "Temps maximum de cache" "Rapport entre l'âge de l'objet dans le cache et son âge sur le site" "Temps minimum de cache" <options>`
- `refresh pattern -i /.*\.trendmicro\.com/.* 180 100% 300 reload-into-ims ignore-reload`

L'option **-i** permet de ne pas tenir compte de la casse des caractères dans l'expression régulière.

La personnalisation sélective de la durée du cache est basée sur la directive `refresh pattern` de Squid. Cette directive permet un contrôle très fin de la validité des objets mis en cache.

Lors d'une requête, Squid décide du comportement à adopter en fonction de l'état de l'objet dans son cache :

- si l'objet n'est pas dans le cache, Squid le demande au serveur qui héberge l'objet, le met en cache et le fournit au client ;
- si l'objet est dans le cache et qu'il est considéré comme étant encore à jour, Squid le fournit directement au client ;
- s'il n'est plus considéré comme à jour, alors une requête `If-modified-since` est envoyée au serveur qui héberge l'objet.

Pour déterminer si un objet est à jour, Squid utilise plusieurs paramètres :

- la valeur liée à l'objet enregistré :
  - **age** correspond au temps en seconde écoulé depuis l'entrée de l'objet dans le cache (objet_age = maintenant - objet_date)
  - **lm_age** correspond à l'age de l'objet au moment de l'entrée dans le cache, temps, en secondes, écoulé entre la dernière modification de l'objet sur le serveur hébergeur et son entrée dans le cache. (lm_age = objet_date - objet_lastmod)
  - **expires** est la date d'expiration de l'objet éventuellement fournie par le serveur hébergeur au moment de l'entrée de l'objet dans le cache. Si elle est renseignée, la valeur de `Temps minimum de cache` prend le pas sur cette valeur.
- la valeur fournie par le client ;

Squid tient compte de la variable **client_max_age** éventuellement fournie par le client, elle indique l'âge maximal de l'objet accepté par le client. Si cette valeur est fournie par le client elle prend le pas sur la valeur `Temps maximum de cache` du fichier de configuration de Squid.

- les valeurs du fichier de configuration de Squid :
  - temps écoulé depuis le téléchargement (**age**), temps maximum et minimum de cache :
    - si `Temps maximum de cache` est défini et que le temps écoulé depuis le téléchargement est supérieur, l'objet est périmé et devra être mis à jour ;
    - si le temps écoulé depuis le téléchargement est inférieur ou égal au `Temps minimum de cache`, l'objet est considéré comme étant à jour.
  - date d'expiration de l'objet fournie par le serveur hébergeur :
    - si la date d'expiration de l'objet (**expires**) est définie par le serveur hébergeur et qu'elle est dépassée, l'objet est périmé et devra être mis à jour ;
    - si la date d'expiration de l'objet (**expires**) est définie par le serveur hébergeur mais qu'elle n'est pas encore dépassée, l'objet est considéré comme étant à jour.
  - rapport (**lm_factor**) entre le temps, en secondes, écoulé depuis l'entrée de l'objet dans le cache et son âge au moment de l'entrée dans le cache :

    Plus le score du rapport entre le temps écoulé depuis l'entrée de l'objet dans le cache et son âge au moment de l'entrée dans le cache (**age**/**lm_age**) est élevé plus l'objet risque d'être périmé :
    - peu de temps écoulé (10) / objet vieux (1000) = rapport faible (0.01) → objet probablement à jour
    - beaucoup de temps écoulé (1000) / objet vieux (1000) = rapport élevé (1) → objet probablement périmé
    - peu de temps écoulé (10) / objet jeune (10) = rapport élevé (1) → objet probablement périmé
    - beaucoup de temps écoulé (1000) / objet jeune (10) = ce cas de figure n'arrive pas car géré par des règles en amont.

    Si le rapport est inférieur au pourcentage (**percent**) saisi dans `Rapport entre l'âge de l'objet dans le cache et son âge sur le site`, l'objet est considéré comme à jour. Diminuer la valeur du pourcentage diminue la probabilité (rapport faible) qu'un objet soit périmé.

Enfin, si aucune règle n'aboutit à considérer l'objet comme étant à jour, celui-ci est considéré comme périmé et devra être mis à jour.

Augmenter le nombre de redirections

Certains sites ont besoin de faire un grand nombres de redirections avant de fournir le contenu souhaité à l'utilisateur.

Par défaut, Squid n'accepte que 10 redirections (variable `forward max tries` du fichier de configuration de Squid) ce qui peut entraîner l'abandon des redirections et donc bloquer l'accès au site.

Il est possible à partir de la version 2.5.2 d'EOLE d'augmenter cette valeur en modifiant la variable

`Nombre maximum de redirections testées` de l'onglet.

Paramètre Half_closed_clients

Certains clients peuvent arrêter leur connexion TCP d'envoi tout en laissant leur connexion de réception ouverte. Parfois,Squid ne peut pas faire la différence entre une connexion à demi-fermée et une connexion entièrement fermée :

- si le paramètre `Half closed clients` est à `On`, les connexions demi-fermée sont maintenues ouvertes jusqu'à ce qu'une erreur de lecture ou d'écriture apparaisse ;
- si le paramètre `Half closed clients` est à `Off`, les connexions sont fermées dès qu'il n'y a plus de données à lire (valeur recommandée sur Squid >= 3.0).

Historiquement paramétrée à `On` sur les modules EOLE, sa valeur par défaut a été passée à `Off` sur les versions d'EOLE >= 2.5.1 depuis avril 2016.

Autres paramètres

L'onglet expert Squid permet de modifier et de fixer un nombre conséquent de paramètres optionnels du fichier de configuration : `/etc/squid3/squid.conf`.

Pour plus d'informations sur la modification de ces paramètres, vous pouvez consulter :

- les exemples de configuration dans le fichier de documentation de Squid : `/usr/share/doc/squid3-common/squid.conf.documented.gz`
- la documentation en ligne des différents paramètres : http://www.squid-cache.org/Doc/config/

Voir aussi...

Onglet Filtrage web : Configuration du filtrage web [p.157]

Outil d'analyse de logs LightSquid [p.232]

3.24. Onglet Proxy authentifié : 5 méthodes d'authentification

EOLE propose un mécanisme d'authentification web via un proxy.

Tous les accès web (HTTP et HTTPS) nécessiteront alors une phase d'authentification.

Cette fonctionnalité offre deux avantages :

- il sera possible de savoir quel utilisateur a accédé à une ressource particulière ;
- il sera possible d'appliquer des politiques de filtrage pour chaque utilisateur.

Pour profiter de cette fonctionnalité, il faut activer l'authentification du proxy dans l'onglet `Authentification` : `Activer l'authentification web (proxy)`.

Cinq méthodes d'authentification sont alors disponibles dans l'onglet `Proxy authentifié`.

Authentification NTLM/SMB

Il s'agit d'une authentification transparente pour les postes utilisateurs Windows intégrés dans un domaine Samba.

Il est possible de configurer plusieurs contrôleurs de domaine dans le cadre de l'authentification NTLM/SMB.

C'est la configuration à choisir si vous disposez d'un serveur pédagogique Scribe et/ou d'un serveur administratif Horus.

La syntaxe pour utiliser le proxy authentifié avec une machine hors domaine est `domaine\login` mais elle ne fonctionne pas avec toutes les versions de navigateurs.

L'authentification NTLM/SMB nécessite l'application de la clé de registre suivante sur les clients Windows Vista et Windows Seven :

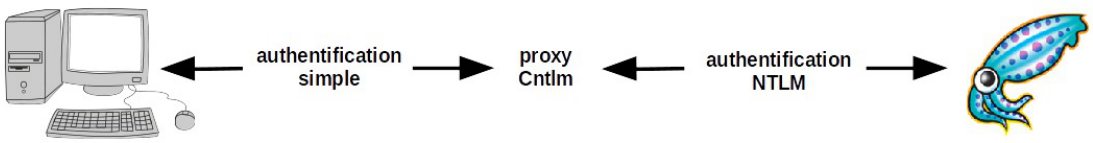
```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa]
"LMCompatibilityLevel"=dword:00000001
```

Pour plus d'informations, consulter : http://technet.microsoft.com/en-us/library/cc960646

Authentification NTLM/SMB poste hors domaine

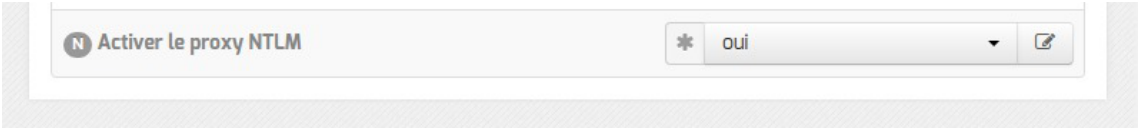
En mode normal, l'authentification NTLM[p.309] peut être facilitée par l'utilisation d'un proxy. Le proxy NTLM proposé par EOLE utilise le logiciel libre Cntlm[p.303].

Le proxy NTLM Cntlm est pré-installé sur les modules Amon, AmonEcole et ses variantes.



Cette méthode permet d'utiliser l'authentification NTLM sur des machines qui ne savent pas le gérer. Ce qui est le cas des machines hors domaine.

Pour activer le proxy NTLM Cntlm il faut passer la variable `Activer le proxy NTLM` à `oui`.



Le port utilisé par défaut par Cntlm est `3127`, il est modifiable en mode expert.

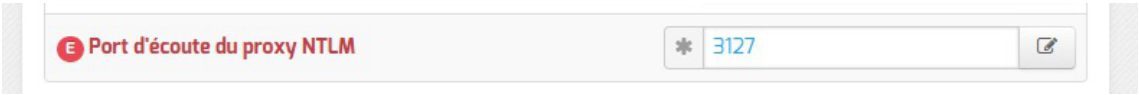
Pour continuer à profiter de l'authentification transparente, les postes intégrés au domaine ne doivent pas passer par Cntlm.

Les postes intégrés au domaine doivent donc utiliser le port `3128` pour passer par le proxy et les postes nomades (hors domaine) doivent utiliser le port `3127` pour passer par Cntlm.

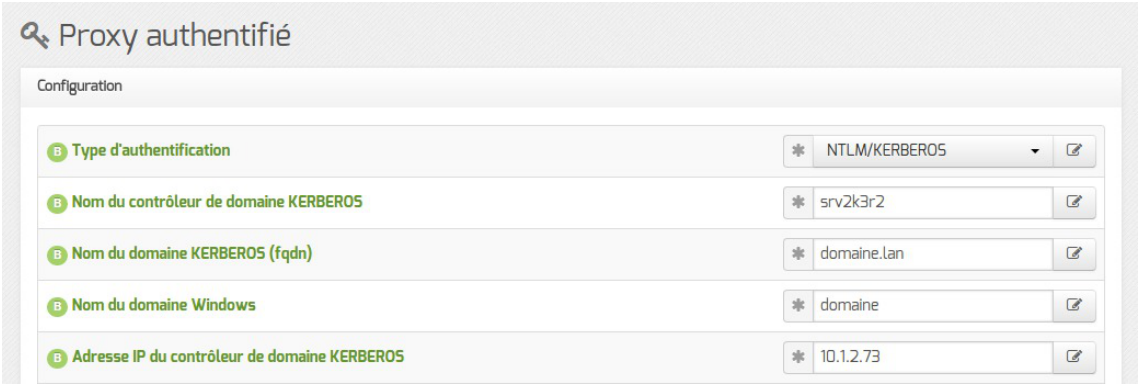
Dans le cas où la découverte automatique du proxy avec WPAD est activée, le port proposé par défaut est automatiquement celui du proxy NTLM Cntlm (`3127` par défaut).

C'est le premier domaine spécifié qui sera utilisé par Cntlm.

En mode expert il est possible de changer le port d'écoute par défaut du proxy NTLM.



Authentification NTLM/KERBEROS



Il s'agit d'une authentification transparente pour les postes utilisateurs Windows intégrés dans un domaine Active Directory.

Cette méthode d'authentification nécessite l'intégration du serveur au royaume Kerberos.

L'intégration peut être réalisée lors de l'instanciation du module en répondant `oui` à la question suivante :

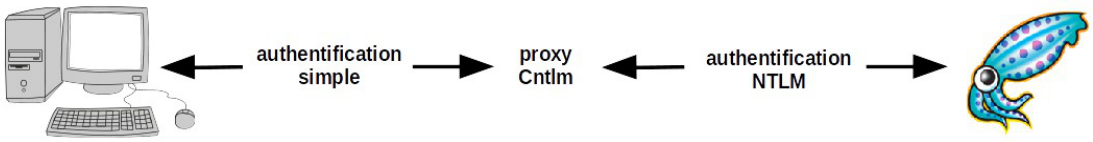
```
Voulez-vous (ré)intégrer le serveur au domaine maintenant ?
```

> Si la configuration de l'authentification NTLM/KERBEROS est réalisée après l'instanciation, il est possible de relancer l'intégration du serveur à tout moment à l'aide du script `enregistrement_domaine.sh`.

Authentification NTLM/KERBEROS poste hors domaine

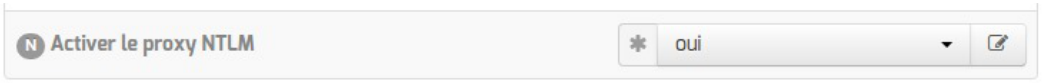
En mode normal, l'authentification NTLM[p.309] peut être facilitée par l'utilisation d'un proxy. Le proxy NTLM proposé par EOLE utilise le logiciel libre Cntlm[p.303].

Le proxy NTLM Cntlm est pré-installé sur les modules Amon, AmonEcole et ses variantes.



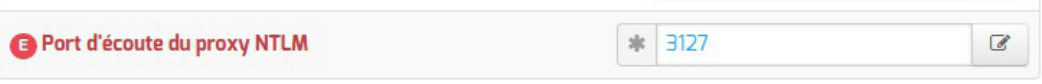
Cette méthode permet d'utiliser l'authentification NTLM sur des machines qui ne savent pas le gérer. Ce qui est le cas des machines hors domaine.

Pour activer le proxy NTLM Cntlm il faut passer la variable `Activer le proxy NTLM` à `oui`.



> Le port utilisé par défaut par Cntlm est `3127`, il est modifiable en mode expert.
>
> Pour continuer à profiter de l'authentification transparente, les postes intégrés au domaine ne doivent pas passer par Cntlm.
>
> Les postes intégrés au domaine doivent donc utiliser le port `3128` pour passer par le proxy et les postes nomades (hors domaine) doivent utiliser le port `3127` pour passer par Cntlm.
>
> Dans le cas où la découverte automatique du proxy avec WPAD est activée, le port proposé par défaut est automatiquement celui du proxy NTLM Cntlm (`3127` par défaut).

En mode expert il est possible de changer le port d'écoute par défaut du proxy NTLM.



Authentification LDAP

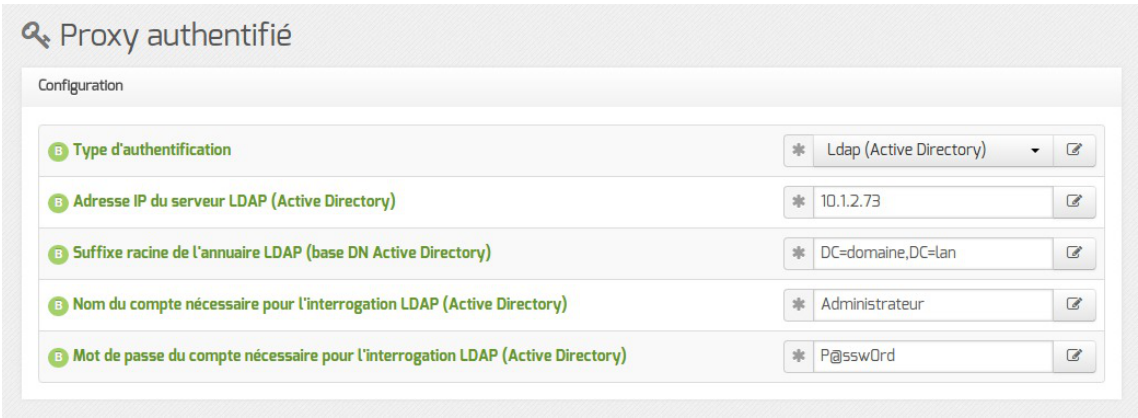
Il s'agit d'une authentification non transparente s'appuyant sur un annuaire de type OpenLDAP.

Ce type d'authentification est recommandé pour les postes hors domaine.

En mode normal, il est possible de déclarer un annuaire de secours.

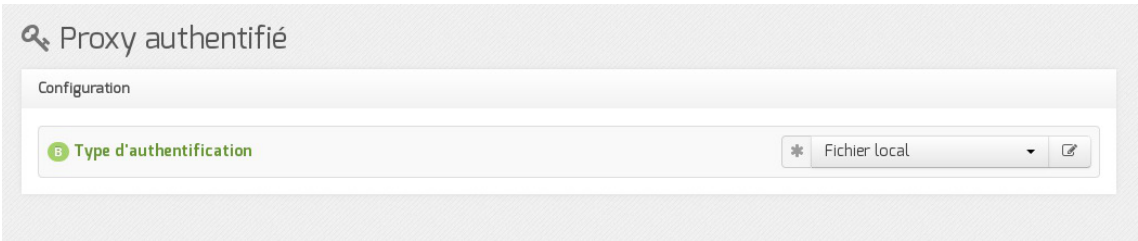
Cet annuaire est interrogé uniquement si le premier ne répond pas.
Cette fonctionnalité est recommandée dans le cas d'annuaires répliqués.

Authentification LDAP (Active Directory)



Il s'agit d'une authentification non transparente s'appuyant sur un annuaire de type Active Directory.
Ce type d'authentification est recommandé pour les postes hors domaine.

Authentification sur Fichier local



Il s'agit d'une authentification non transparente s'appuyant sur un fichier de comptes locaux.
Ce type d'authentification peut être utilisé dans une petite structure, comme une école, qui ne disposerait pas vraiment d'un réseau local.

Pour cette authentification, le fichier utilisé par défaut est : `/etc/squid3/users`
Il doit être au format *htpasswd* et il peut être peuplé en utilisant la commande suivante :

```
# htpasswd -c /etc/squid3/users <compte>
```

En mode conteneur (module AmonEcole par exemple), le fichier `/etc/squid3/users` se trouve dans le conteneur `proxy` :

```
# ssh proxy
# htpasswd -c /etc/squid3/users <compte>
```

ou

```
# CreoleRun "htpasswd -c /etc/squid3/users <compte>" proxy
```

Désactivation de l'authentification sur une interface

Pour chacune des interfaces (hors eth0 si plusieurs interfaces sont configurées), il est possible d'activer/désactiver l'authentification proxy.

Par exemple, pour désactiver l'authentification proxy uniquement sur le réseau eth2, il faut aller dans l'onglet `Interface-2` et répondre `non` à la question `Activer l'authentification sur cette interface (s'applique aussi aux VLAN)`.

3.25. Onglets Squid2 et Proxy authentifié 2 : Double authentification

Par double authentification, nous entendons la possibilité de pouvoir configurer deux types distincts d'authentification proxy.

Par exemple, pouvoir utiliser à la fois une authentification NTLM/SMB et une authentification LDAP.

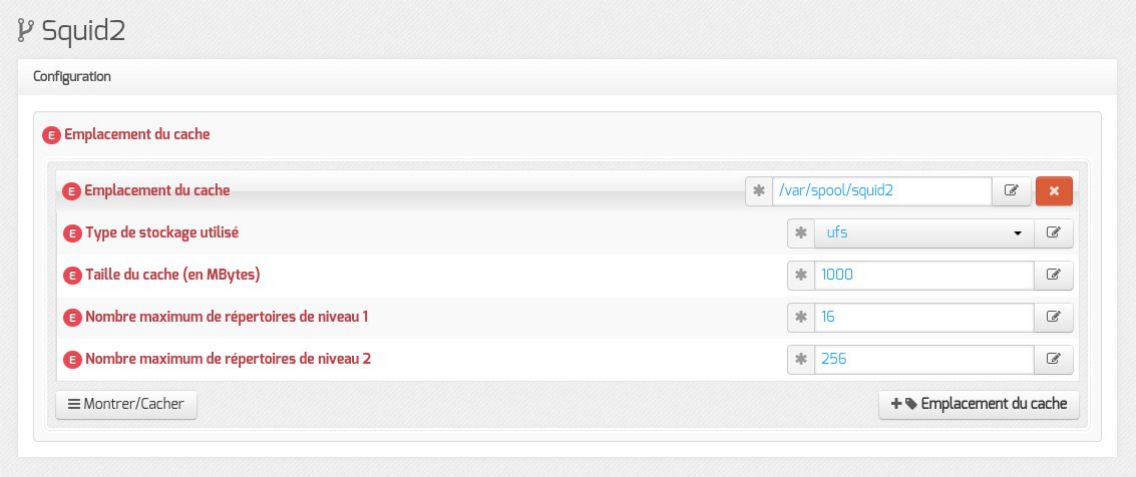
L'implémentation retenue est d'utiliser une instance du logiciel Squid par type d'authentification.

Configuration pas à pas

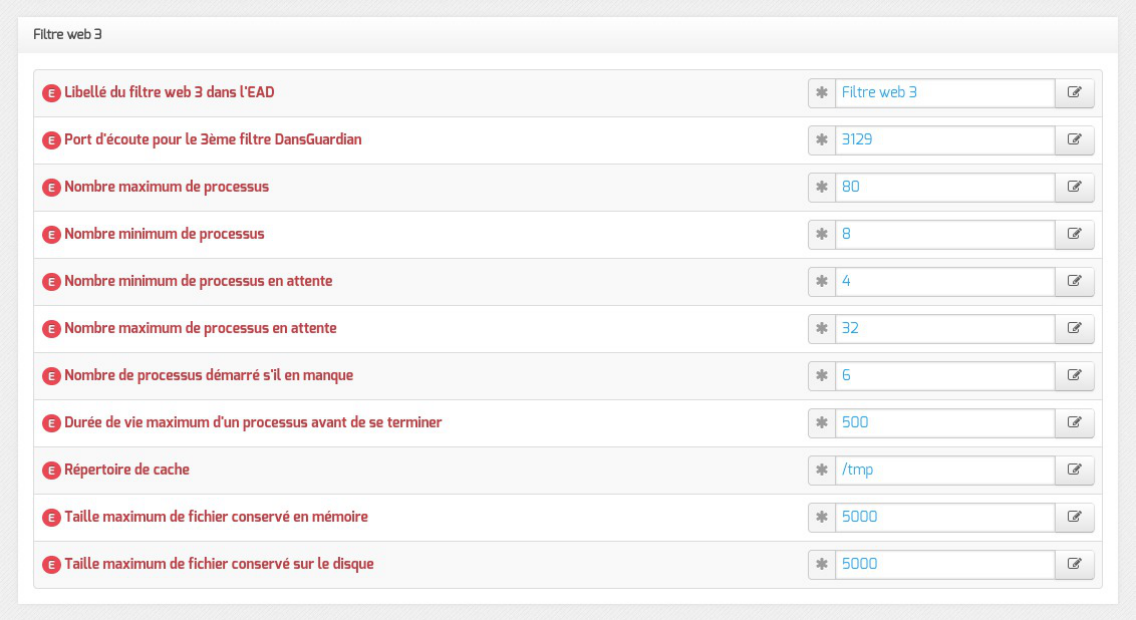
1. Activation de la deuxième instance de Squid dans l'onglet `Authentification` :

2. Configuration du type d'authentification dans l'onglet `Proxy authentifié 2` :

3. Paramétrage de la seconde instance de Squid dans l'onglet expert `Squid2` :



4. Paramétrage du filtrage web associé dans l'onglet expert `Filtrage web` (section `Filtre web 3`)



Notes techniques

Les fichiers de logs spécifiques au second type d'authentifications sont les suivants :

- `/var/log/rsyslog/local/squid/squid2.info.log`
- `/var/log/rsyslog/local/e2guardian/e2guardian2.info.log`

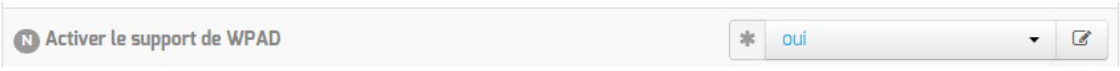
Dans l'état actuel, ces logs ne sont pas consultables au travers de l'interface EAD et seule la première configuration proxy est distribuée par WPAD (voir partie dédiée).

3.26. Onglet Wpad : découverte automatique du proxy

WPAD est mise à disposition sur les modules Amon et ses variantes (AmonEcole, ...) au travers du paquet `eole-wpad` mais n'est fonctionnel que si le paquet `eole-proxy` est installé.

Pour fonctionner correctement, il faut que l'URL `wpad.<nom_domaine_local>` correspondre à l'adresse IP du serveur web.

Le support de WPAD doit être activé et correctement configuré sur le module Amon.



Activation de WPAD dans l'onglet Services

Dans l'onglet `Services` de l'interface de configuration du module `Activer le support de WPAD` doit être placé à `oui`.

Vue de l'onglet Wpad dans l'interface de configuration du module

Cela rend disponible l'onglet `Wpad` au sein duquel le `Nom de domaine du service WPAD` doit être rempli avec la même valeur que le `Nom de domaine privé du réseau local` présent dans l'onglet `Général`.

Si vous souhaitez utiliser un autre nom de domaine qui ne correspondrait pas au `Nom de domaine privé du réseau local` de l'onglet `Général`, il faut le déclarer dans le champ `Nom domaine local supplémentaire ou rien` de l'onglet `Zones-dns`.

Pour être pris en compte, les changements doivent être enregistrés et suivis de la commande `reconfigure` sur le module.

WPAD supporte les VLAN et les alias, Nginx renvoie le bon fichier WPAD si des VLAN ou des alias sont déclarés.

En mode expert, Il est également possible de changer le port du proxy diffusé par défaut pour une interface, un VLAN ou un alias donné.

Voir aussi...

Configurer la découverte automatique du proxy avec WPAD [p.197]

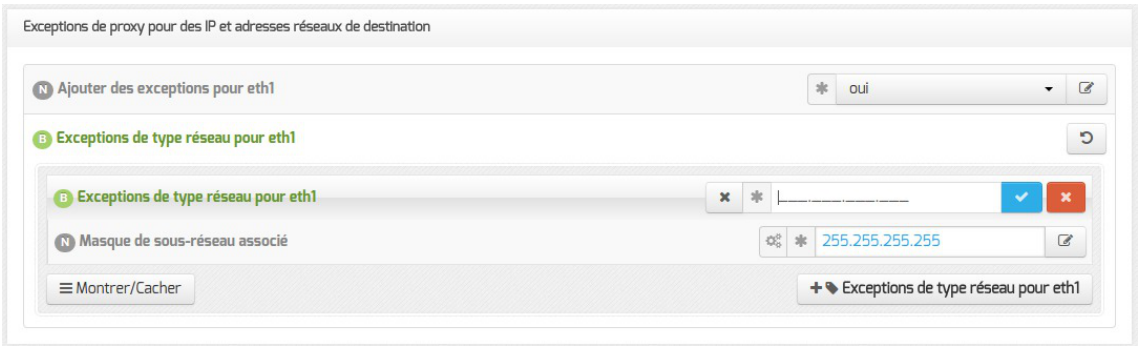
3.27. Onglet Exceptions proxy

Dans l'onglet `Exceptions proxy` de l'interface de configuration du module il est possible d'ajouter des exclusions dans la configuration automatique du proxy.

Il est possible de déclarer différents types d'exceptions.

Exception sur une adresse IP ou une plage d'adresses IP

Cette exception commune à ERA et à WPAD permet de déclarer une adresse IP ou une plage d'adresses IP de destination pour laquelle on ne passe pas par le proxy.



Le bouton `Exceptions de type réseau pour eth-n` permet d'ajouter plusieurs exceptions sur une même interface.

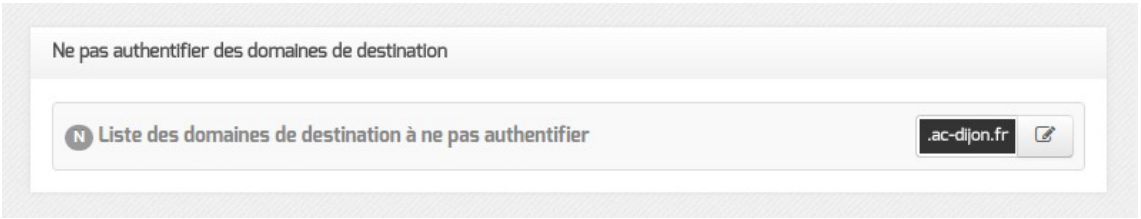
Exception sur un nom de domaine

Cette exception commune à ERA et à WPAD permet de déclarer un domaine de destination pour lequelle on ne passe pas par le proxy.

Il est possible d'ajouter plusieurs exceptions sur une même interface.

Exception au niveau de l'authentification des domaines

Cette exception permet de déclarer des sites pour lesquels le proxy ne demandera pas l'authentification à l'utilisateur qui souhaite y accéder.



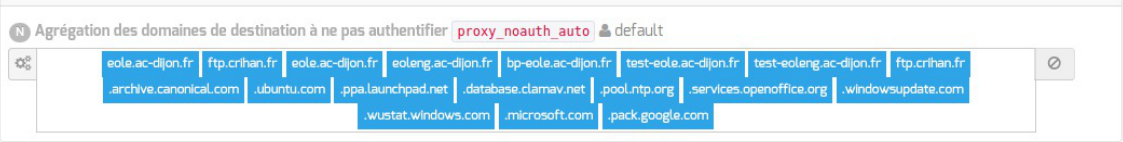
Si cNTLM et WPAD sur activés sur l'interface réseau, les utilisateurs utiliseront directement Squid (sans passer par cNTLM) pour accéder à ces sites.

Les domaines commençants par un `.` sont gérés, le domaine lui-même et les sous-domaines ne sont pas authentifiés.

Si on spécifie la valeur `.ac-dijon.fr` alors `ac-dijon.fr` et `www.ac-dijon.fr` seront autorisés sans authentification.

Une liste de sites à ne pas authentifier par défaut est stockée dans la variable cachée `proxy_noauth_auto`.

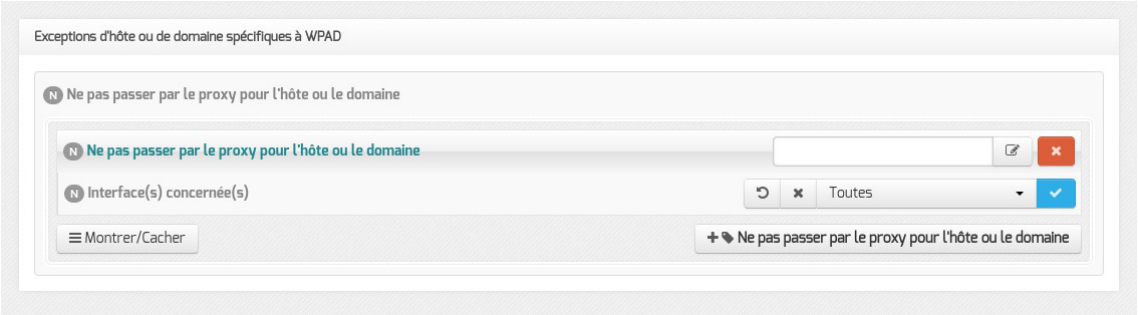
Il est possible de l'afficher dans l'onglet `Exceptions proxy` de l'interface de configuration du module en activant le mode Debug.



Cette variable reprend la liste des sites qui étaient dans le template `domaines_noauth` des versions EOLE antérieures à 2.5.2.

Exception sur un nom d'hôte (spécifique à WPAD)

L'exception sur un nom d'hôte s'effectue sur le nom d'hôte et sur le nom d'hôte complet.



Il faut choisir une interface ou toutes les interfaces sur lesquelles l'exception sera appliquée. Le bouton `+ Ne pas passer par le proxy pour l'hôte ou le domaine` permet d'ajouter plusieurs exceptions sur une même interface.

Ce type d'exception étant spécifique à WPAD, il n'est pas prise en compte par les autres services gérant des exceptions au niveau du proxy.

Si le champ `Ne pas passer par le proxy pour l'hôte ou le domaine` a comme valeur `www.ac-monacad.fr`, le fichier WPAD.dat généré contiendra la ligne `|| localHostOrDomainIs(host, "www.ac-monacad.fr")` qui permet d'exclure simplement des URLs.

Compléments sur `Ne pas passer par le proxy pour le` domaine (dnsDomainIs) :

http://findproxyforurl.com/netscape-documentation/#dnsDomainIs

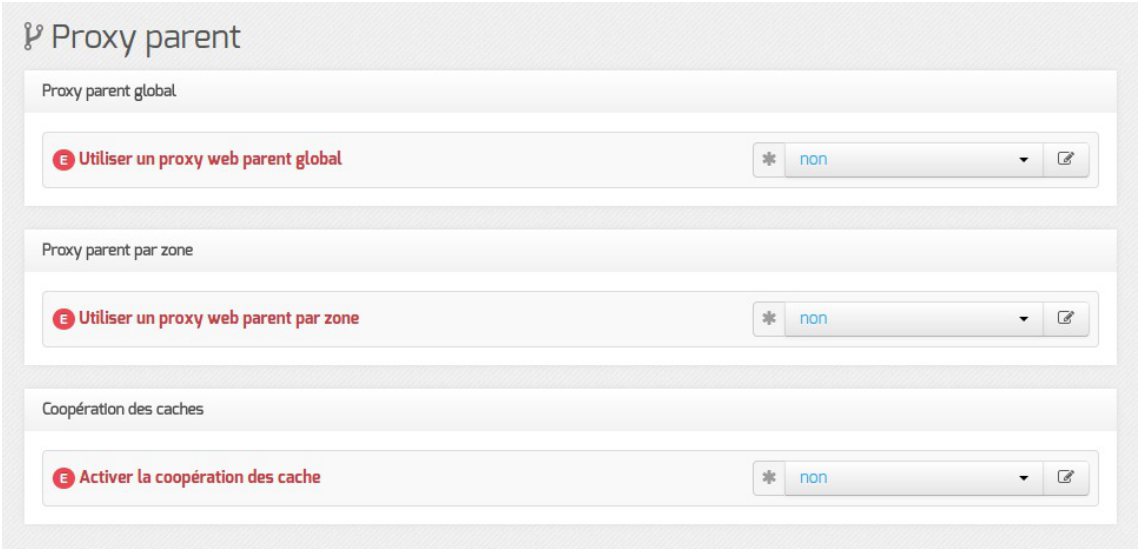
Compléments sur `Ne pas passer par le proxy pour l'hôte ou le domaine` (localHostOrDomainIs) :

http://findproxyforurl.com/netscape-documentation/#localHostOrDomainIs

3.28. Onglet Proxy parent : Chaînage du proxy

L'onglet expert `Proxy parent` permet de déclarer un ou plusieurs serveurs proxy à utiliser en amont de celui activé sur le module EOLE.

Cette fonctionnalité est à utiliser dans le cas de la mise en place d'un proxy centralisé au niveau d'une académie ou d'un groupe d'établissements.



Vue de l'onglet Proxy-pere de l'interface de configuration du module

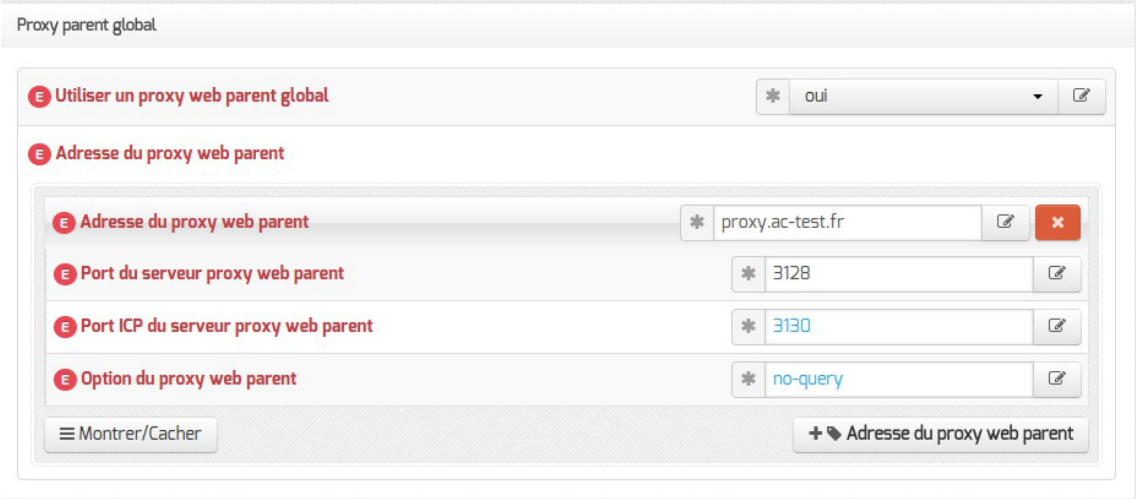
Si plusieurs proxy parents sont déclarés, un mécanisme de type round-robin[p.312] est utilisé afin de répartir la charge sur les différents serveurs.

Les proxy déclarés ici ne seront pas utilisés par le serveur lui-même.

La déclaration d'un proxy à utiliser par le module EOLE s'effectue dans l'onglet `Général` en passant la variable : `Utiliser un serveur mandataire (proxy) pour accéder à Internet` à `oui`.

Proxy parent global

Le ou les proxy parents peuvent être déclarés de façon globale en passant la variable `Utiliser un proxy web parent global` à `oui`.



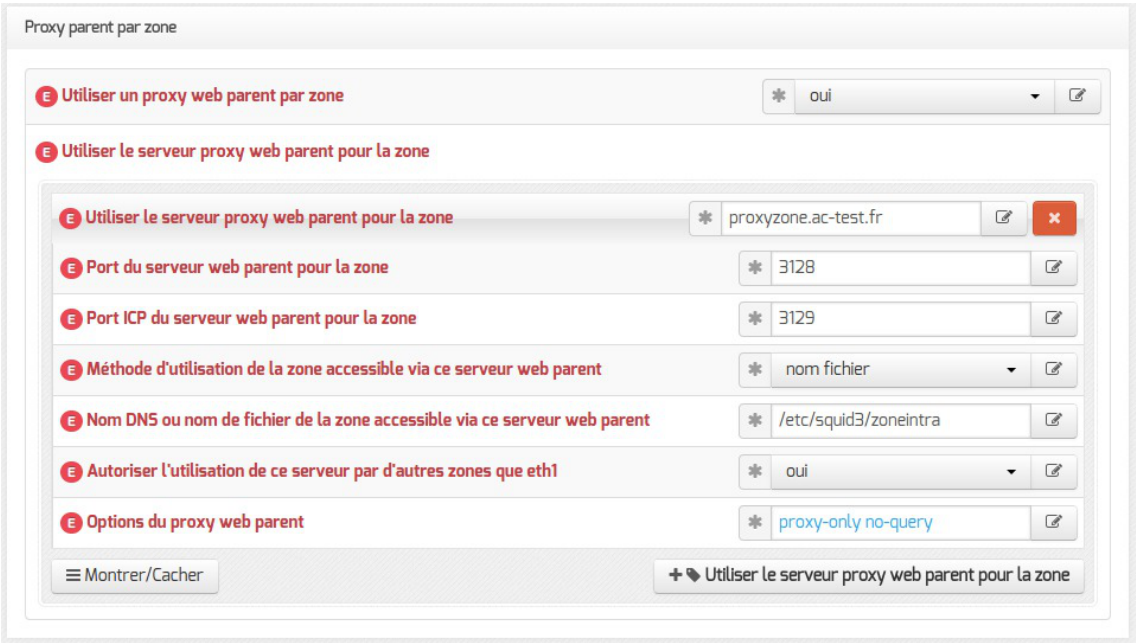
Vue de l'onglet Proxy-pere de l'interface de configuration du module

Proxy parent par zone

Pour des besoins spécifiques, des proxy parents peuvent être déclarés pour des zones DNS particulières en passant la variable `Utiliser un proxy web parent par zone` à `oui`.

Les zones DNS de destination peuvent être :

- soit renseignées directement dans la variable `Nom DNS ou nom de fichier de la zone accessible via ce serveur web parent` si la `Méthode d'utilisation de la zone accessible via ce serveur web parent` est `DNS` ;
- soit renseignées dans un fichier texte dont le chemin est à indiquer dans la variable `Nom DNS ou nom de fichier de la zone accessible via ce serveur web parent` si la `Méthode d'utilisation de la zone accessible via ce serveur web parent` est `nom fichier` ;



Vue de l'onglet Proxy-pere de l'interface de configuration du module

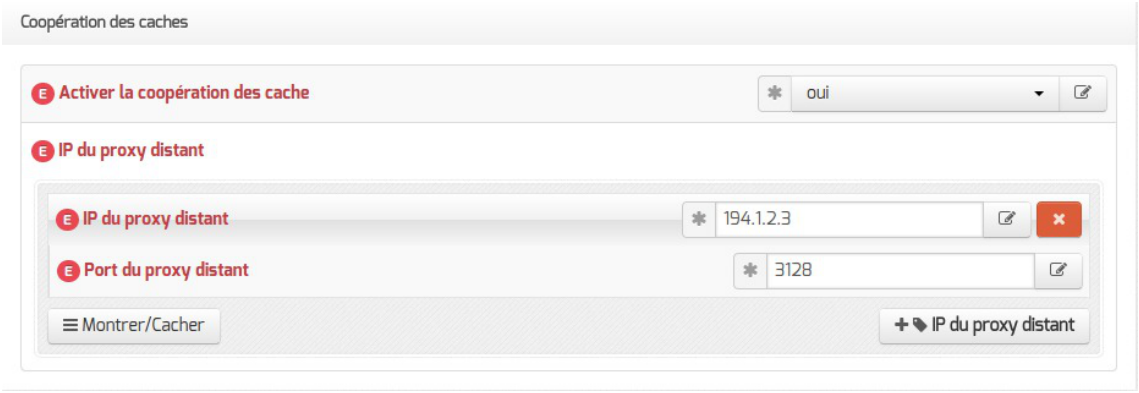
Pour que ces sous-domaines soient également pris en compte, le nom DNS du domaine doit

> impérativement être précédé d'un point.
>
> Il est possible de renseigner directement plusieurs zones DNS en les séparant par des espaces, exemple : `.domain1 .domain2 .domain3`.

Coopération des caches

Si on a plusieurs proxy cache, il peut être intéressant de les faire collaborer pour partager le cache.

Cela se fait via le mécanisme de proxy sibling[p.311].



Vue de l'onglet Proxy-pere de l'interface de configuration du module

3.29. Onglet Reverse proxy : Configuration du proxy inverse

EOLE propose un serveur proxy inverse (reverse proxy) basé sur le logiciel libre Nginx[p.308].

Le proxy inverse est un type de serveur proxy, habituellement placé en frontal de serveurs web, qui permet de relayer des requêtes web provenant de l'extérieur vers les serveurs internes (situés en DMZ[p.304] par exemple). Cela le différencie grandement d'un proxy classique comme Squid[p.313].

Concrètement, le proxy inverse permet d'ouvrir des services web installés sur des serveurs situées "derrière" le pare-feu l'accès sur Internet sans avoir recours à des règles *iptables/DNAT*.

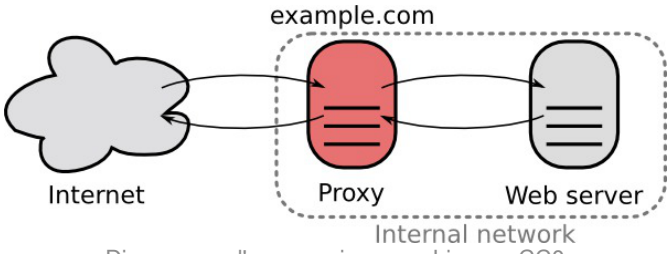
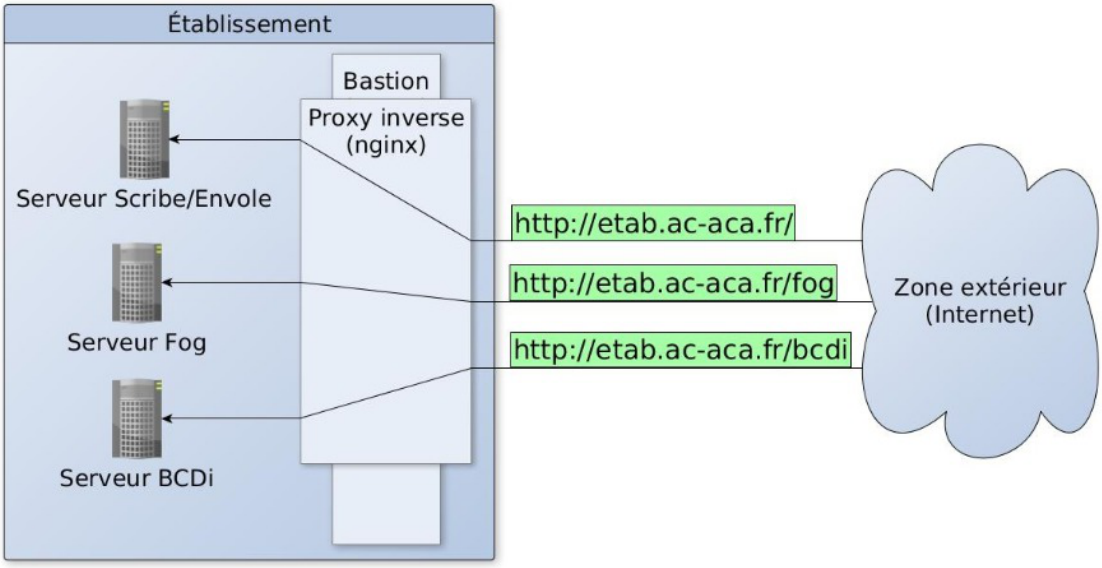


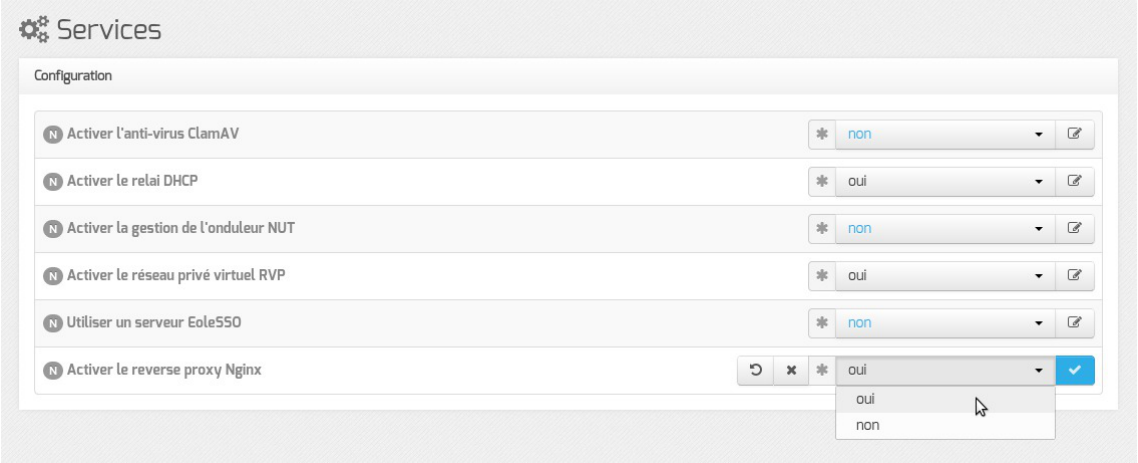
Diagramme d'un proxy inverse - Licence CC0

Le proxy inverse EOLE peut relayer des requêtes vers les services suivants :

- les serveurs EoleSSO ;
- les EAD ;
- le serveur d'administration d'Envole ;
- le protocole HTTP[p.306] ;
- le protocole HTTPS[p.306].



Avant toute chose, le proxy inverse doit être activé dans l'onglet `Services` en passant `Activer le reverse proxy Nginx` à `oui`.



Vue de l'onglet Services de l'interface de configuration du module

L'activation du service fait apparaître un nouvel onglet.

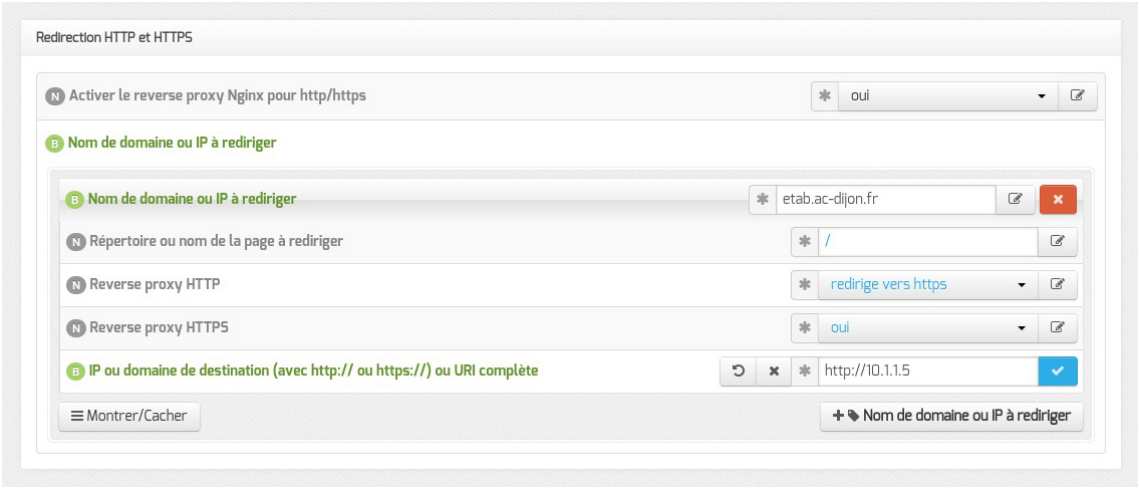
Vue de l'onglet Reverse proxy de l'interface de configuration du module

Redirection de services particuliers

Pour rediriger le service EoleSSO (port 8443) il faut indiquer l'adresse IP ou le nom de domaine interne de la machine de destination (adresse IP ou le nom de domaine interne du module Scribe). Si le service EoleSSO est activé localement il est impossible de réaliser une redirection pour ce service.

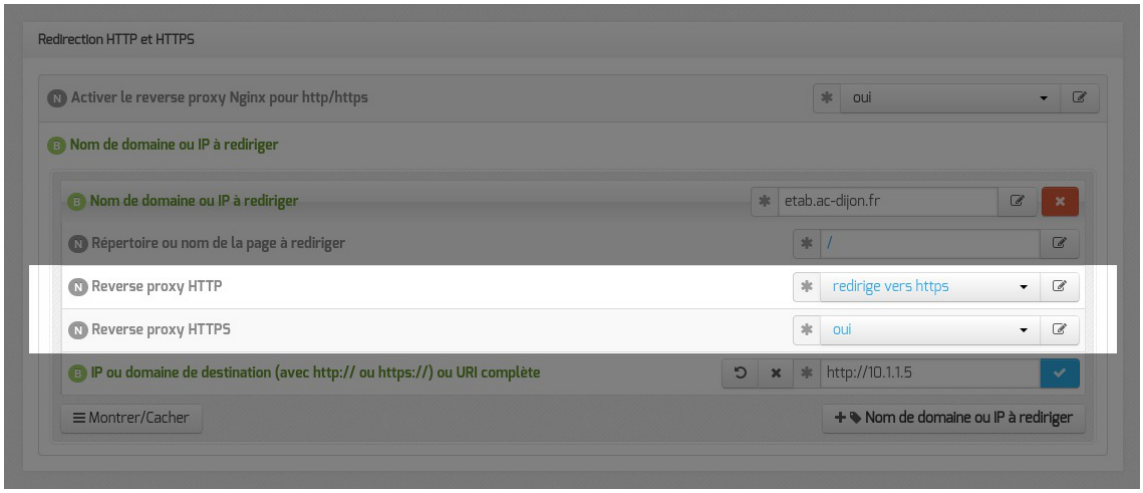
Le service SSO local du module Amon ne devra pas être activé si vous renseignez l'adresse d'un service SSO distant au niveau du proxy inverse.

Redirection HTTP et HTTPS



Pour rediriger HTTP et HTTPS il est nécessaire de passer la variable `Activer le reverse proxy Nginx pour le http/https` à `oui` et de renseigner plus d'informations :

- le `Nom de domaine ou IP à rediriger` : le nom de domaine diffusé auprès des utilisateurs. Ce nom de domaine est celui qui permet d'accéder au module Amon ou AmonEcole ;
- le `Répertoire ou nom de la page à rediriger` permet de rediriger un sous-répertoire vers une machine. La valeur par défaut est `/` ;
- l'`IP ou domaine de destination (avec http:// ou https://) ou URI complète` permet de saisir l'adresse IP (exemple : `http://192.168.10.1`), le nom de domaine (exemple : `http://scribe.monetab.fr`) ou l'URI[p.314] (exemple : `http://scribe.monetab.fr/webmail/`) du serveur de destination hébergeant la ou les applications.



Il est possible de forcer l'utilisation du protocole HTTPS pour les requêtes utilisant le protocole HTTP de façon transparente. De cette manière, un utilisateur web se connectant à l'adresse `http://monetab.fr` sera automatiquement redirigé vers `https://monetab.fr`

Ainsi les communications sont automatiquement chiffrées protégeant la transmission de données sensibles (nom d'utilisateur, mot de passe, etc.).

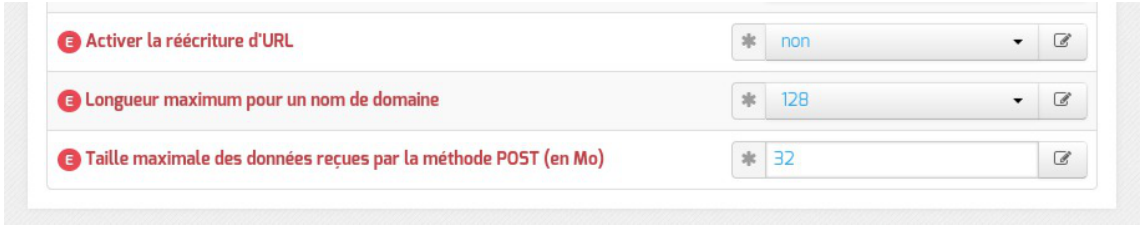
Le proxy inverse peut être utilisé pour ne rediriger que le HTTPS en passant les valeurs `Reverse proxy HTTP` à `non` et `Reverse proxy HTTPS` à `oui`.

Il est possible d'ajouter plusieurs redirections en cliquant sur le bouton `Nom de domaine ou IP à rediriger`.

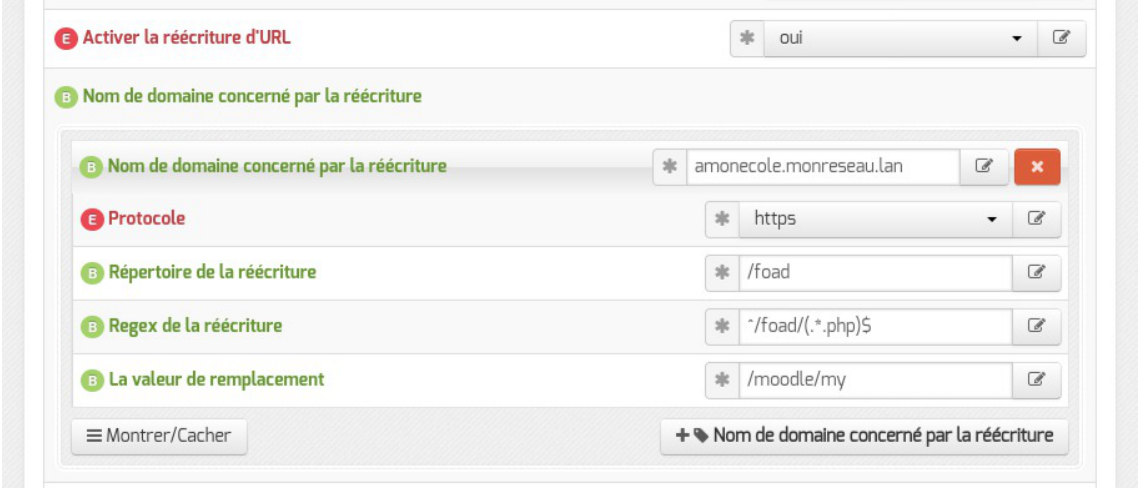
> Un répertoire déterminé peut également être redirigé vers un serveur différent. Par exemple le lien vers l'application Pronote[p.311], `https://monetab.fr/pronote/` peut être redirigé vers `http://pronote.monetab.fr/` (attention, le "/" final est important, puisqu'il faut rediriger à la racine du serveur de destination).

En mode expert il est possible :

- d'`Activer la réécriture d'URL` ;
- d'augmenter ou de diminuer la `Longueur maximum pour un nom de domaine` ;
- de choisir la `Taille maximale des données reçues par la méthode POST (en Mo)`.



L'activation de la réécriture d'URL permet d'ajouter une expression rationnelle et une valeur de remplacement.



Il n'y a pas de lien automatique entre une "redirection" Nginx renseignée et une réécriture d'URL.

Pour que la réécriture d'URL s'applique à une règle il faut que le nom de domaine, le protocole et le répertoire de la réécriture correspondent au paramètres saisis dans la règle de "redirection" renseignée.

Sur une installation recevant de très nombreuses connexions, diminuer la valeur de la `Longueur maximum pour un nom de domaine` (server_names_hash_bucket_size) pourra améliorer les performances du proxy inverse. La valeur optimale varie d'une installation à l'autre.

Avec une valeur trop basse, le service Nginx refusera de démarrer et affichera un message d'erreur ressemblant à :

`could not build the server_names_hash, you should increase server_names_hash_bucket_size: 32`

Nginx Optimization : http://nginx.org/en/docs/http/server_names.html#optimization

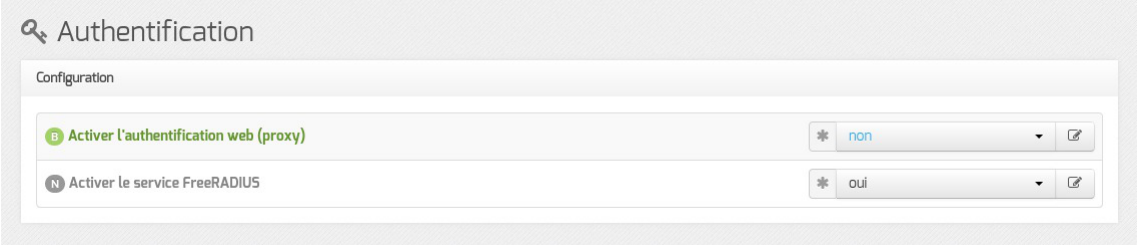
L'option du mode expert `Taille maximale des données reçues par la méthode POST (en Mo)` permet de spécifier la taille des données HTTP au delà de laquelle Nginx renverra une erreur (message : `Request Entity Too Large`).

Dans le cas où, sur un module, le service `eole-web` est installé en plus du service `eole-reverseproxy` (ce qui est le cas sur le module AmonEcole et ses dérivés), le paramétrage de cette option est déplacée dans l'onglet `Apache`. Sa valeur est alors utilisée à la fois pour le serveur web Apache et pour le proxy inverse Nginx.

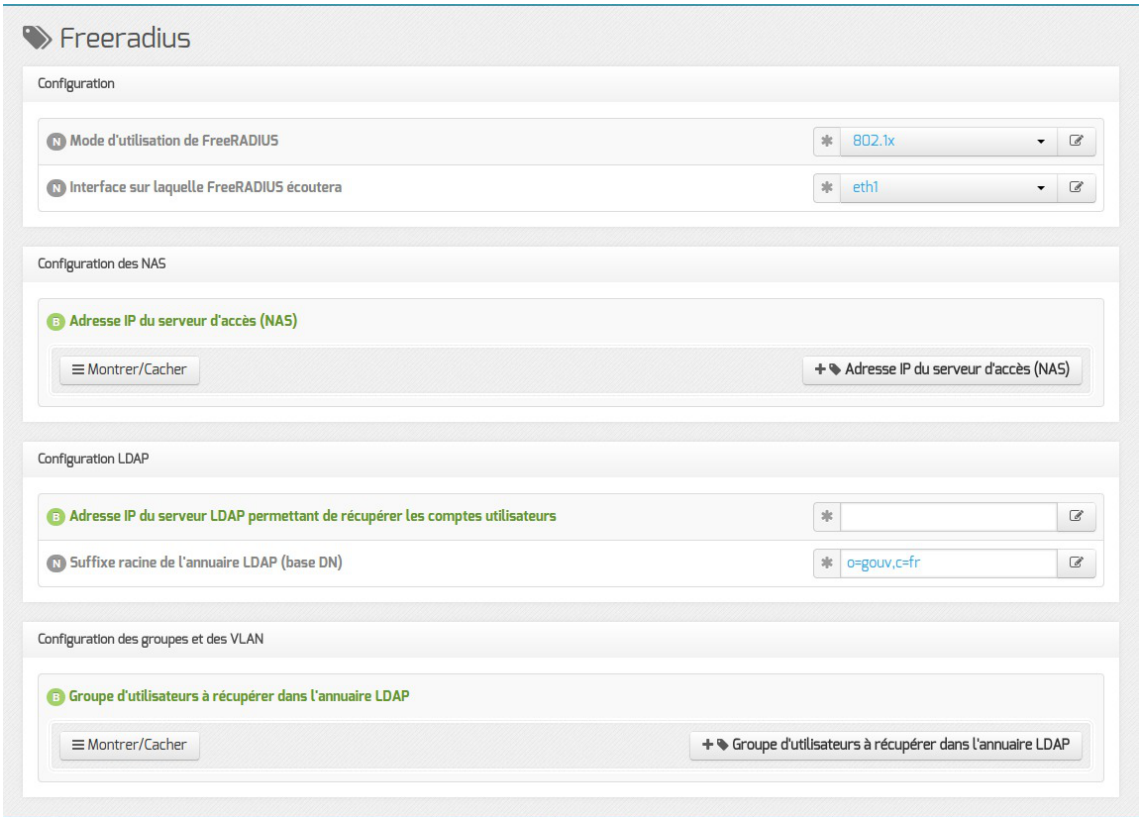
3.30. Onglet Freeradius : Configuration de l'authentification Radius

EOLE propose un mécanisme d'authentification réseau basé sur le protocole RADIUS[p.312].

Pour profiter de cette fonctionnalité, il faut activer le service d'authentification RADIUS en passant `Activer le service FreeRADIUS` à `oui` dans l'onglet `Authentification`.



Cela fera apparaître l'onglet `Freeradius`.



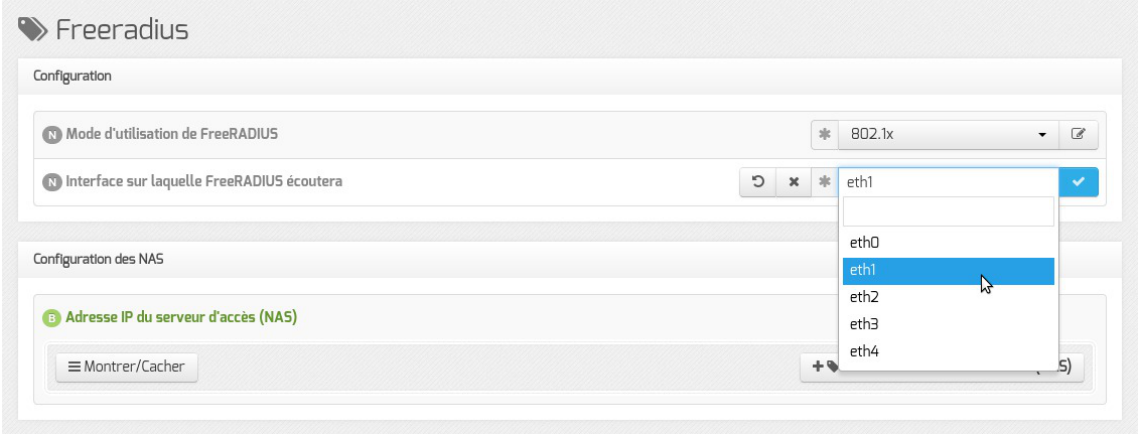
Vue de l'onglet Freeradius de l'interface de configuration du module

Il est possible de choisir entre 2 modes d'utilisation de FreeRADIUS :

- 802.1x ;
- accounting.

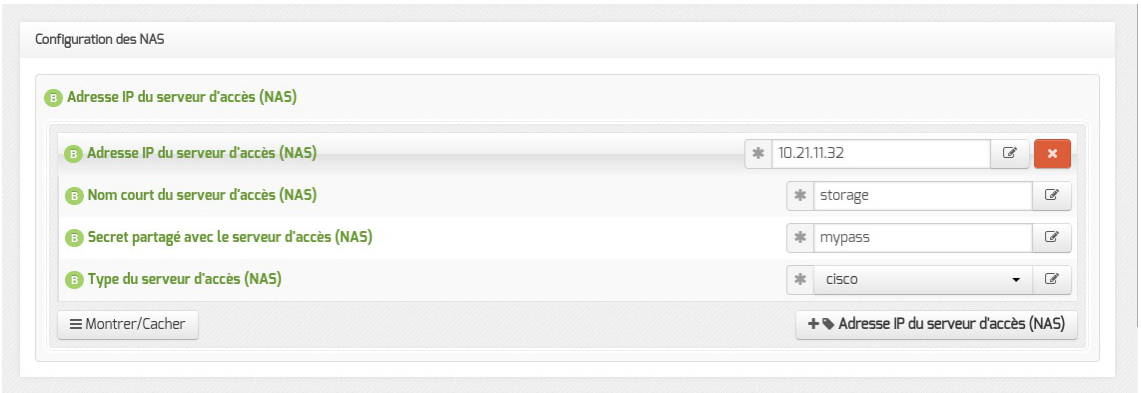
Le mode 802.1x

Le mode `802.1x` permet de taguer dynamiquement des ports d'un switch (NAS[p.308]) sur lesquels sont brassées des stations en fonction du compte LDAP de connexion.



`Interface sur laquelle FreeRADIUS écoutera` : définition de l'interface d'écoute de FreeRADIUS.

Configuration des NAS



`Adresse IP du serveur d'accès (NAS)` : adresse IP du switch.

`Nom court du serveur d'accès (NAS)` : libellé du switch.

`Secret partagé avec le serveur d'accès (NAS)` : secret partagé entre FreeRADIUS et le switch.

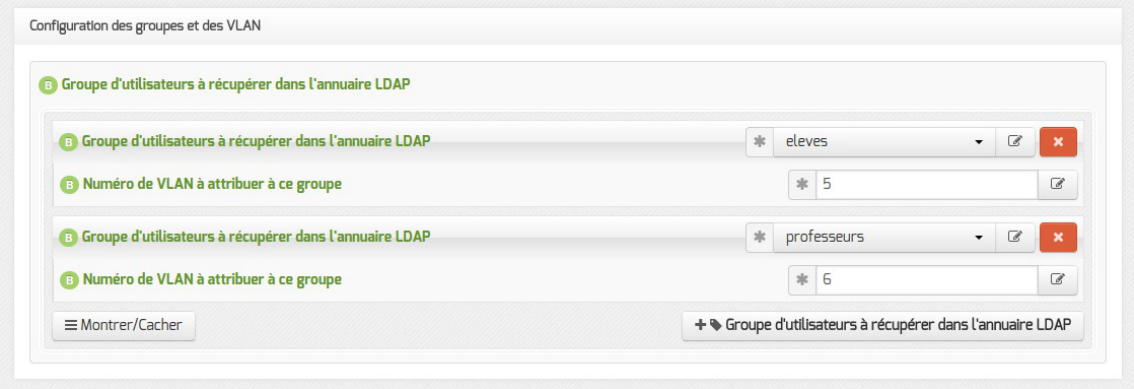
`Type du serveur d'accès (NAS)` : type de switch.

Configuration LDAP

`Adresse IP du serveur LDAP permettant de récupérer les comptes utilisateurs` : adresse IP LDAP.

`Suffixe racine de l'annuaire LDAP (base DN)` : *ou=education,o=gouv,c=fr* par exemple.

Configuration des groupes et des VLAN



`Groupe d'utilisateurs à récupérer dans l'annuaire LDAP` : saisir ou choisir un groupe existant dans l'annuaire.

`Numéro de VLAN à attribuer à ce groupe` : les machines se connectant avec un utilisateur appartenant au groupe indiqué ci-dessus verra son port tagué sur ce numéro de VLAN.

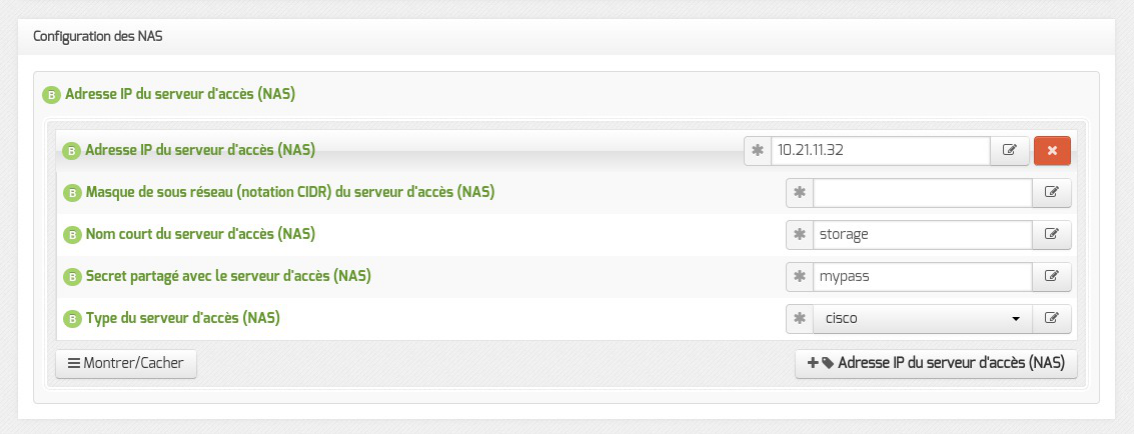
Le mode accounting

Le mode accounting permet de créer un réseau Wi-Fi WPA enterprise sur une borne Wi-Fi (NAS) ayant pour identifiants autorisés les compte/motDePasse de l'annuaire LDAP déclaré.

Onglet Freeradius - mode accounting

`Adresse IP sur laquelle FreeRADIUS écoutera` : l'adresse IP d'une des interfaces du serveur.

Configuration des NAS



Onglet Freeradius - mode accounting

`Adresse IP du serveur d'accès (NAS)` : adresse IP de la borne Wi-Fi.

`Masque de sous réseau (notation CIDR) du serveur d'accès (NAS)` : 24 (en notation

CIDR[p.302]) si le réseau est de classe C.

`Nom court du serveur d'accès (NAS)` : libellé de la borne Wi-Fi.

`Secret partagé avec le serveur d'accès (NAS)` : secret partagé entre FreeRADIUS et la borne Wi-Fi.

`Type du serveur d'accès (NAS)` : type de borne (other en général).

Configuration LDAP

Onglet Freeradius - mode accounting

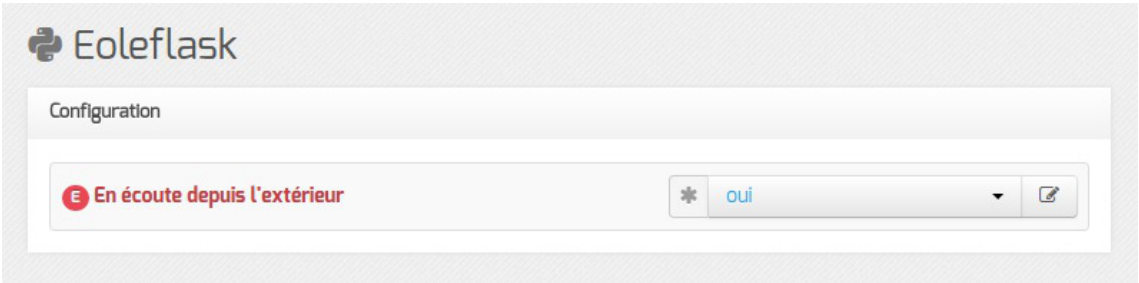
`Adresse IP du serveur LDAP permettant de récupérer les comptes utilisateurs` : adresse IP ldap.

`Suffixe racine de l'annuaire LDAP (base DN)` : *ou=education,o=gouv,c=fr* par exemple.

`Clé d'accès reader à la base ldap sur Scribe (/root/.reader)` : à récupérer sur le serveur LDAP.

3.31. Onglet Eoleflask

Dans cet onglet se trouvent les options concernant le service Eoleflask et les options des applications reposant sur ce service.



Passer la variable `En écoute depuis l'extérieur` à `oui` permet d'accéder à l'interface de configuration du module depuis un poste client.

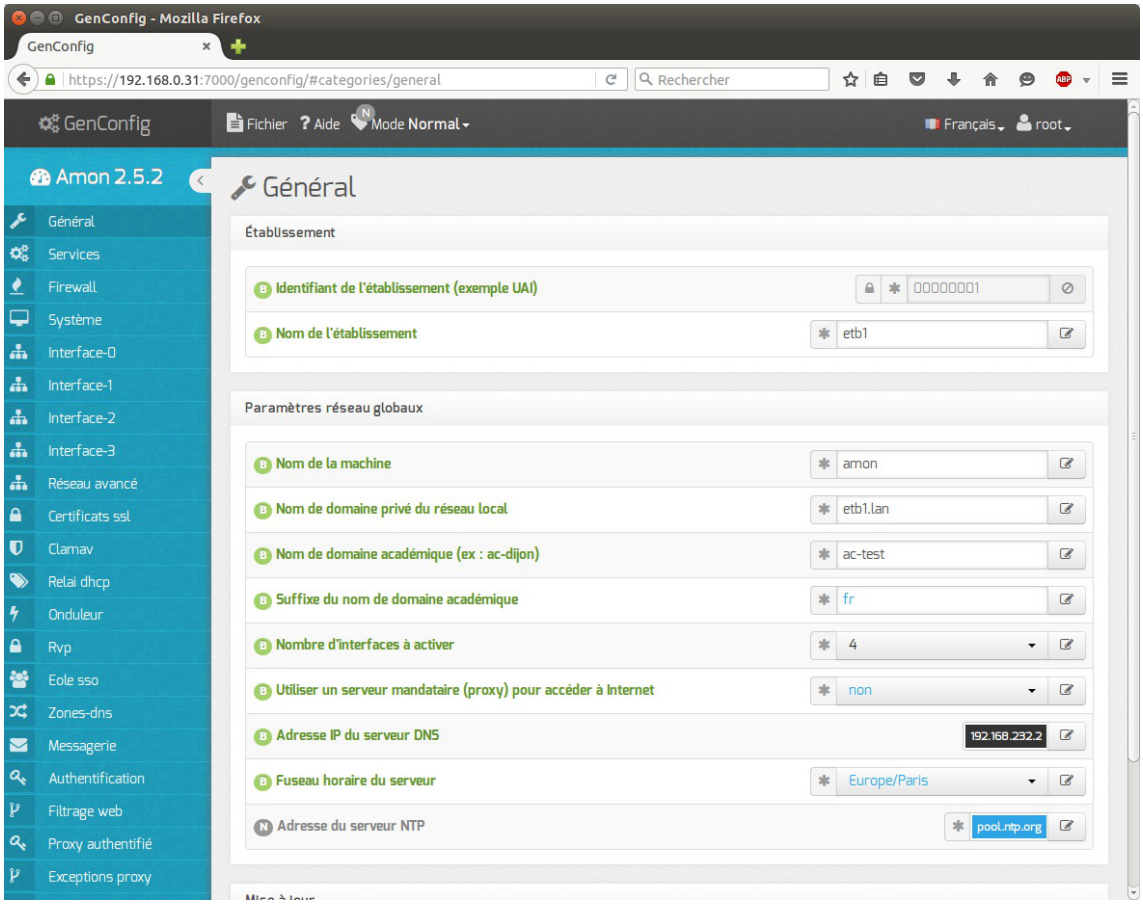
Accès distant

Après instance ou reconfigure, si votre adresse IP est autorisée pour l'administration du serveur, l'interface de configuration du module est accessible depuis un navigateur web en HTTPS à l'adresse suivante :

`https://<adresse_serveur>:7000/genconfig/`

Ne pas oublier d'utiliser le protocole HTTPS et de préciser le numéro de port 7000.

Il faut ensuite valider les certificats pour pouvoir accéder à l'interface.



Vue de l'interface de configuration au travers d'un navigateur web

Pour autoriser l'accès distant à une ou plusieurs adresses IP il faut le déclarer explicitement dans l'onglet `Interface-n` de l'interface de configuration du module en passant la variable `Autoriser les connexions SSH` à `oui`.

4. Configuration du module Amon avec le module Scribe en DMZ

L'installation d'un module Scribe et plus généralement de serveurs pédagogiques dans une DMZ[p.304] permet de les isoler d'attaques provenant de l'intérieur (par exemple des services saturés par un virus utilisant le broadcast[p.302]) et de les placer dans une zone où l'accès aux autres réseaux de l'établissement doit être explicitement autorisé.

L'utilisation d'une DMZ vise également à faciliter l'ouverture de services sur Internet, et notamment les services web (portail de l'établissement, messagerie, logiciels de vie scolaire, ...) et l'accès FTP.

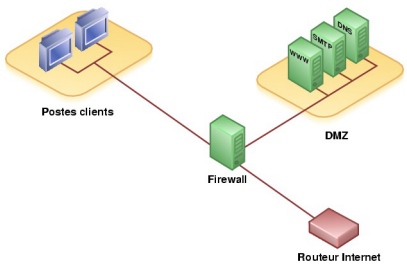


Diagramme d'une DMZ

Ports à ouvrir

Pour permettre un bon fonctionnement du serveur Scribe dans une DMZ, certains ports demandent à être ouverts.

Ces ports servent à la communication entre le serveur et les stations clientes, notamment pour le protocole Samba et pour le service Scribe (client Scribe) :

- 137-139 (TCP/UDP) : Samba ;
- 445 (TCP) : Samba ;
- 8788 (TCP) : service Scribe (client Scribe) ;
- 5800/5900 (TCP) : VNC.

Par défaut, sur le module Amon, une DMZ peut se connecter sur Internet.

Il faut cependant faire de la traduction d'adresse réseau (NAT[p.308]) pour assurer le trafic.

Si la communication entre la DMZ et l'extérieur est fermée, les ports à ouvrir sont :

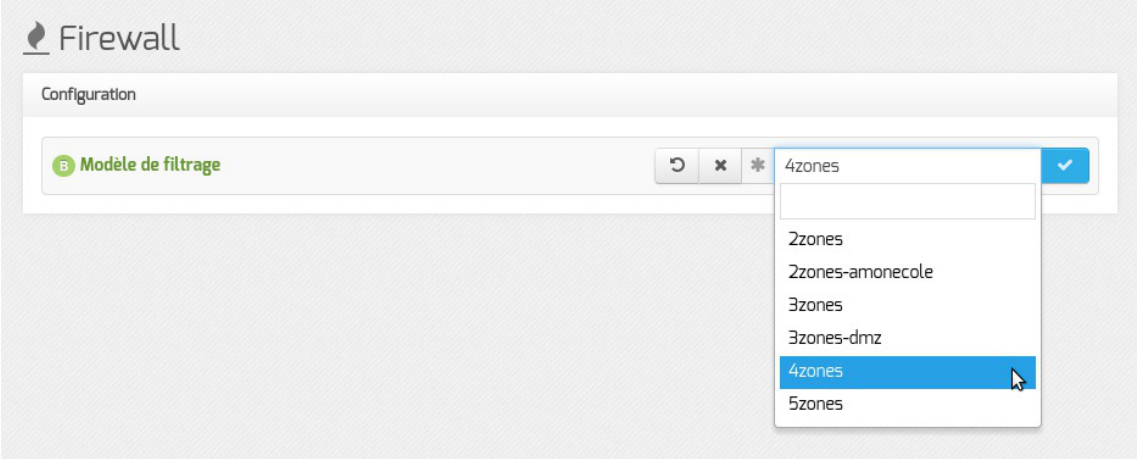
- pour le serveur Zéphir : 22 (TCP), 7080 (TCP) et 8090 (TCP) ;
- pour les serveurs mises à jour : 80 (TCP) ;
- pour les bases de données antivirales : tous les ports vers les adresses `database.clamav.net` et `cvd.clamav.net`

Pour pouvoir accéder au serveur Scribe depuis l'extérieur par le web et par le FTP, il faut rediriger la connexion effectuée sur les ports 21 et 443 (HTTP sécurisé) depuis l'extérieur sur le serveur Amon vers le serveur Scribe.

Configuration automatique

Par défaut, le module Amon propose des modèles de pare-feu facilitant la mise en place d'un serveur Scribe en DMZ. Pour configurer le pare-feu, il faut dans l'onglet Firewall, choisir un `Modèle de filtrage` compatible :

- **3zones-dmz** : gestion d'une zone pedago sur eth1 et d'une zone DMZ publique pouvant accueillir un module Scribe sur eth2 ;
- **4zones** : gestion d'une zone admin sur eth1, d'une zone pedago sur eth2 et d'une zone DMZ publique pouvant accueillir un module Scribe sur eth3 ;
- **5zones** : gestion d'une zone admin sur eth1, d'une zone pedago sur eth2, d'une zone DMZ publique pouvant accueillir un module Scribe sur eth3 et d'une zone DMZ privée sur eth4.



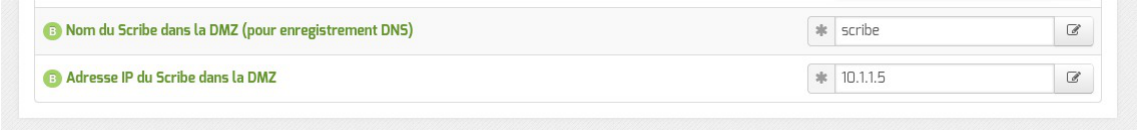
Le modèle de zones proposées correspond à un modèle de filtrage ERA. Les modèles de filtrage ERA sont la description de pare-feu enregistrés dans des fichiers XML situés par défaut dans le répertoire `/usr/share/era/modeles/`.

Avec ERA il est possible de créer un nouveau modèle personnalisé dans le répertoire `/usr/share/era/modeles/`. Celui-ci apparaîtra dans la liste des modèles proposés par défaut.

Ces modèles requièrent que le serveur Scribe soit déclaré au niveau du module Amon.

Pour se faire, dans l'onglet `Firewall` en mode normal ou expert, il faut répondre `oui` à la question `Activer la gestion d'un Scribe dans la DMZ`.

Cela entraîne l'apparition de nouvelles variables permettant de déclarer le nom et l'adresse IP du module Scribe.

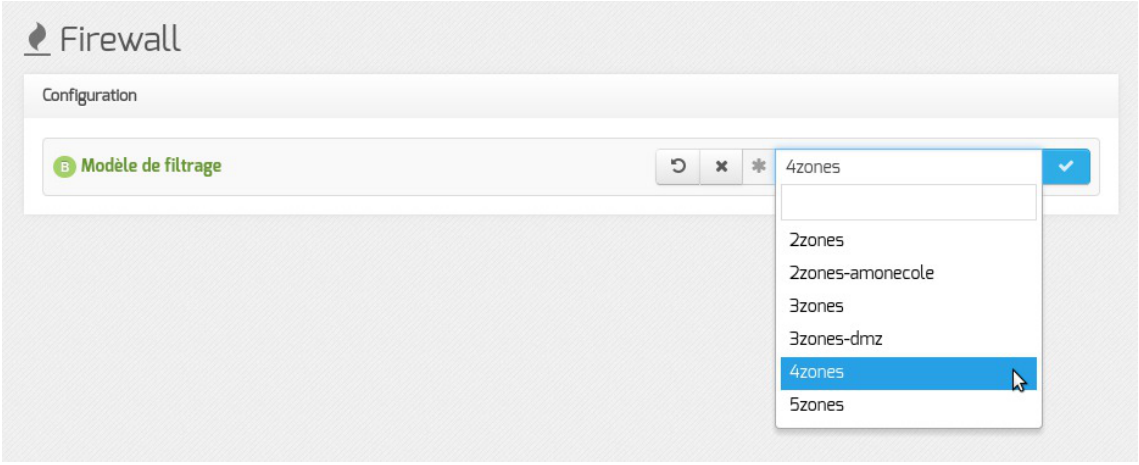


Si le module Scribe offre un service DHCP pour le réseau pédagogique, il faudra activer et configurer le relai du DHCP entre ce serveur et le réseau pédagogique.

Par défaut, le module Amon propose des modèles de pare-feu facilitant la mise en place d'un serveur Scribe en DMZ. Pour configurer le pare-feu, il faut dans l'onglet `Firewall`, choisir un `Modèle de filtrage` compatible :

- **3zones-dmz** : gestion d'une zone pedago sur eth1 et d'une zone DMZ publique pouvant accueillir un module Scribe sur eth2 ;
- **4zones** : gestion d'une zone admin sur eth1, d'une zone pedago sur eth2 et d'une zone DMZ publique pouvant accueillir un module Scribe sur eth3 ;
- **5zones** : gestion d'une zone admin sur eth1, d'une zone pedago sur eth2, d'une zone DMZ publique

pouvant accueillir un module Scribe sur eth3 et d'une zone DMZ privée sur eth4.



Le modèle de zones proposées correspond à un modèle de filtrage ERA. Les modèles de filtrage ERA sont la description de pare-feu enregistrés dans des fichiers XML situés par défaut dans le répertoire `/usr/share/era/modeles/`.

Avec ERA il est possible de créer un nouveau modèle personnalisé dans le répertoire `/usr/share/era/modeles/`. Celui-ci apparaîtra dans la liste des modèles proposés par défaut.

Voir aussi...

- Onglet Relai DHCP [p.57]
- ERA, éditeur de règles pour le module Amon [p.235]

5. Configurer le module Amon pour Envole

Pour un fonctionnement optimal des applications web hébergées sur le module Scribe derrière un serveur Amon ou hébergées sur module AmonEcole, il est impératif d'utiliser un nom de domaine[p.309] (exemple : `monetab.ac-acad.fr`). Celui-ci doit être résolvable depuis Internet et il faut le renseigner partout où cela est nécessaire.

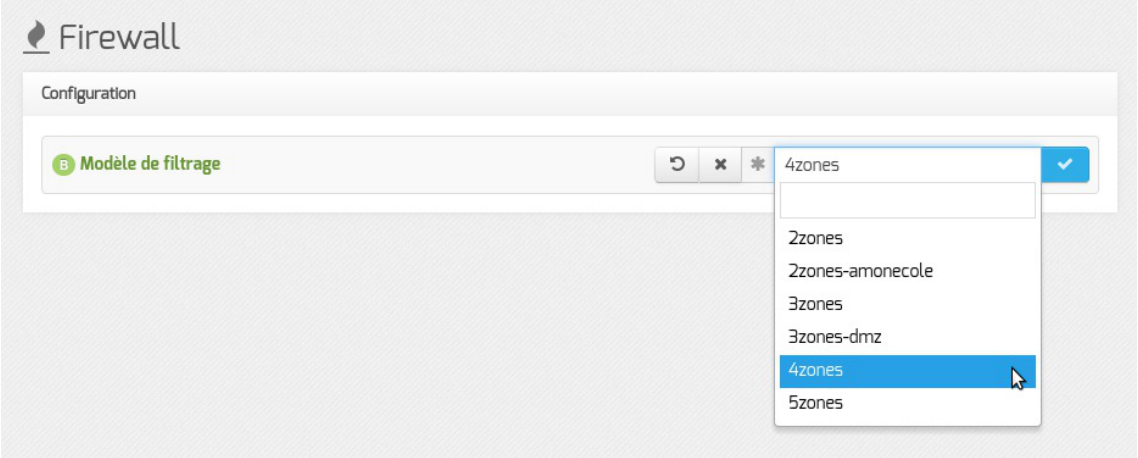
Ce nom de domaine sera à utiliser tant depuis l'extérieur de l'établissement que depuis l'intérieur.

Pour rendre accessible Envole ou certaines applications web hébergées sur le module Scribe depuis l'extérieur, il faut activer et configurer le pare-feu et le proxy inverse.

Configurer le pare-feu

Par défaut, le module Amon propose des modèles de pare-feu facilitant la mise en place d'un serveur Scribe en DMZ. Pour configurer le pare-feu, il faut dans l'onglet `Firewall`, choisir un `Modèle de filtrage` compatible :

- **3zones-dmz** : gestion d'une zone pedago sur eth1 et d'une zone DMZ publique pouvant accueillir un module Scribe sur eth2 ;
- **4zones** : gestion d'une zone admin sur eth1, d'une zone pedago sur eth2 et d'une zone DMZ publique pouvant accueillir un module Scribe sur eth3 ;
- **5zones** : gestion d'une zone admin sur eth1, d'une zone pedago sur eth2, d'une zone DMZ publique pouvant accueillir un module Scribe sur eth3 et d'une zone DMZ privée sur eth4.

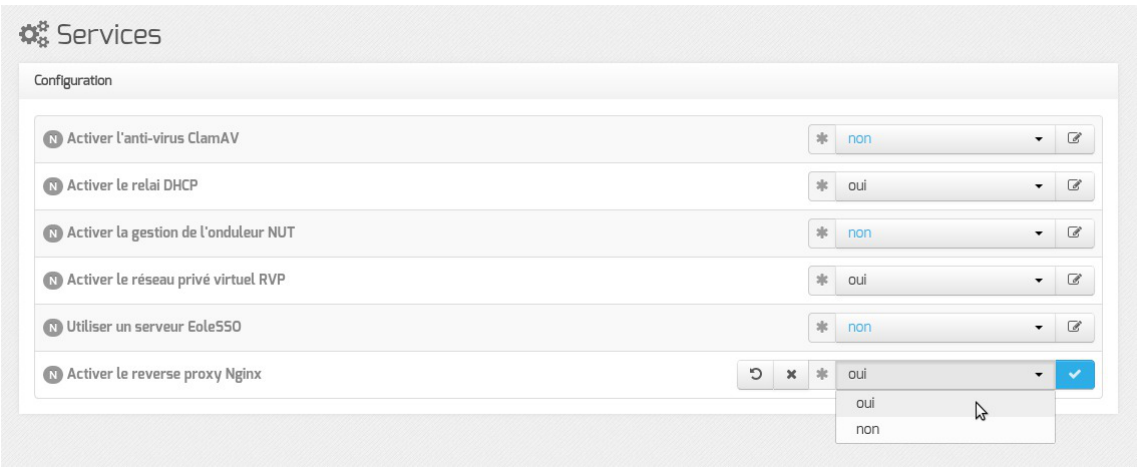


Le modèle de zones proposées correspond à un modèle de filtrage ERA. Les modèles de filtrage ERA sont la description de pare-feu enregistrés dans des fichiers XML situés par défaut dans le répertoire `/usr/share/era/modeles/`.

Avec ERA il est possible de créer un nouveau modèle personnalisé dans le répertoire `/usr/share/era/modeles/`. Celui-ci apparaîtra dans la liste des modèles proposés par défaut.

Configuration du proxy inverse

Pour activer le proxy inverse, dans `Services`, passer `Activer le reverse proxy Nginx` à `oui`.



Vue de l'onglet Services de l'interface de configuration du module

L'activation du service fait apparaître un nouvel onglet nommé `Reverse proxy`.

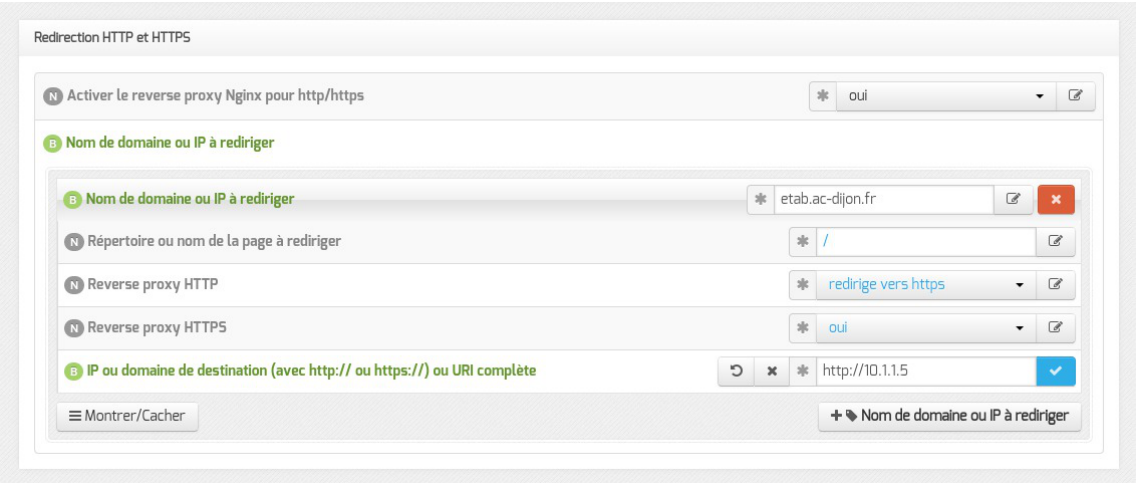
Vue de l'onglet Reverse proxy de l'interface de configuration du module

Redirection de services particuliers

Pour rediriger le service EoleSSO (port 8443) il faut indiquer l'adresse IP ou le nom de domaine interne de la machine de destination (adresse IP ou le nom de domaine interne du module Scribe). Si le service EoleSSO est activé localement il est impossible de réaliser une redirection pour ce service.

Le service SSO local du module Amon ne devra pas être activé si vous renseignez l'adresse d'un service SSO distant au niveau du proxy inverse.

Redirection HTTP et HTTPS

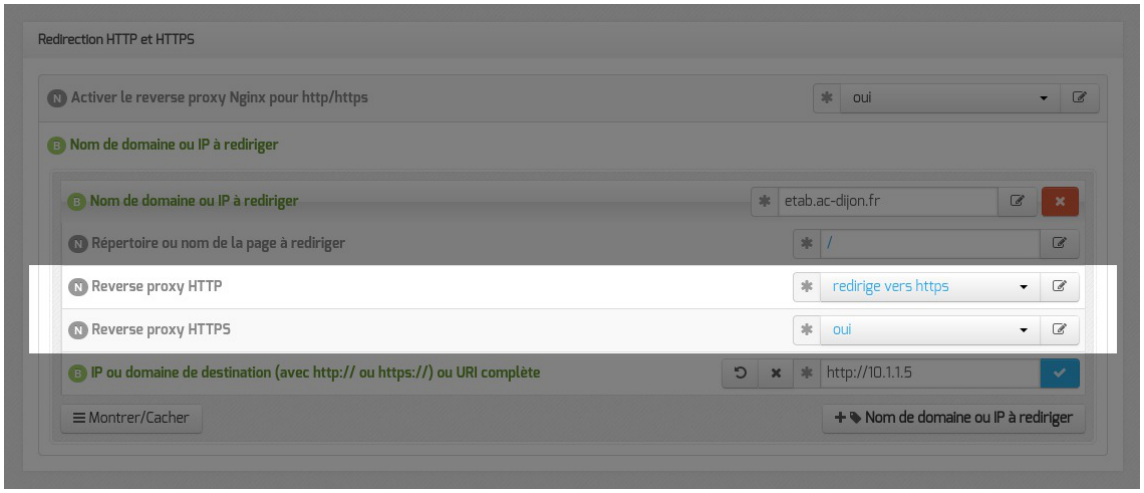


Pour rediriger HTTP et HTTPS il est nécessaire de passer la variable `Activer le reverse proxy Nginx pour le http/https` à `oui` et de renseigner plus d'informations :

- le `Nom de domaine ou IP à rediriger` : le nom de domaine diffusé auprès des utilisateurs. Ce nom de domaine est celui qui permet d'accéder au module Amon ou AmonEcole ;
- le `Répertoire ou nom de la page à rediriger` permet de rediriger un sous-répertoire vers

une machine. La valeur par défaut est `/` ;

- l'`IP ou domaine de destination (avec http:// ou https://) ou URI complète` permet de saisir l'adresse IP (exemple : `http://192.168.10.1`), le nom de domaine (exemple : `http://scribe.monetab.fr`) ou l'URI[p.314] (exemple : `http://scribe.monetab.fr/webmail/`) du serveur de destination hébergeant la ou les applications.



Il est possible de forcer l'utilisation du protocole HTTPS pour les requêtes utilisant le protocole HTTP de façon transparente. De cette manière, un utilisateur web se connectant à l'adresse `http://monetab.fr` sera automatiquement redirigé vers `https://monetab.fr`

Ainsi les communications sont automatiquement chiffrées protégeant la transmission de données sensibles (nom d'utilisateur, mot de passe, etc.).

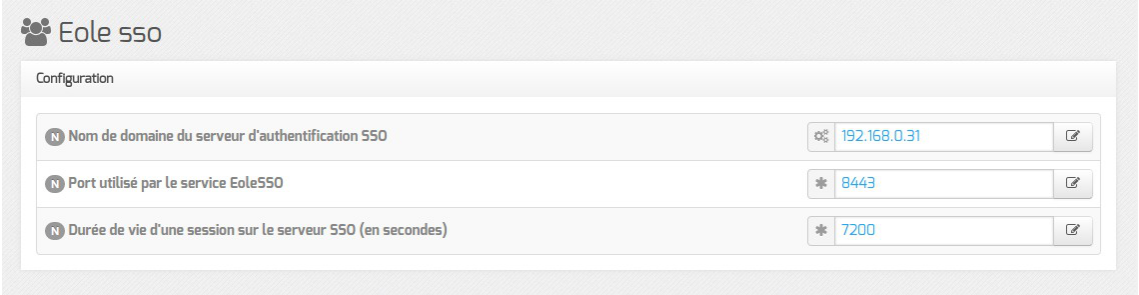
Le proxy inverse peut être utilisé pour ne rediriger que le HTTPS en passant les valeurs `Reverse proxy HTTP` à `non` et `Reverse proxy HTTPS` à `oui`.

Il est possible d'ajouter plusieurs redirections en cliquant sur le bouton `Nom de domaine ou IP à rediriger`.

Un répertoire déterminé peut également être redirigé vers un serveur différent. Par exemple le lien vers l'application Pronote[p.311], `https://monetab.fr/pronote/` peut être redirigé vers `http://pronote.monetab.fr/` (attention, le "/" final est important, puisqu'il faut rediriger à la racine du serveur de destination).

Activation de l'authentification unique

Si vous voulez activer le service EoleSSO sur le module Amon, `Utiliser un serveur EoleSSO à distant` dans l'onglet `Services`, dans l'onglet `Eole sso`, seuls les paramètres `Nom de domaine du serveur d'authentification SSO` et `Port utilisé par le service EoleSSO` sont requis et les autres options ne sont pas disponibles car elles concernent le paramétrage du serveur local.



L'option `Nom de domaine du serveur d'authentification SSO` doit être configurée avec le nom de domaine public utilisé dans Envole (typiquement : *monetab.ac-monacad.fr*).

Dans ce cas l'utilisateur `admin` du module Scribe sera administrateur du module Amon.

Dans le cas de l'utilisation du serveur EoleSSO local, `Nom de domaine du serveur d'authentification SSO` doit être renseigné avec le nom DNS du serveur.

Nom de domaine et récapitulatif de la configuration

Le nom de domaine doit être renseigner à de multiples endroits de la configuration.

- onglet `Général` : choisir le modèle de filtrage ;
- onglet `Services` :
  - Activer le proxy inverse Nginx : `oui` ;
- onglet `Eole sso` :
  - Nom de domaine du serveur d'authentification SSO : `etab.ac-acad.fr` ;
- onglet `Applications web` si module AmonEcole :
  - Nom de domaine des applications web (sans http://) : `etab.ac-acad.fr` ;
- onglet `Reverse proxy` :
  - Nom de domaine par défaut : `etab.ac-acad.fr` ;
  - Nom de domaine du serveur SSO : `etab.ac-acad.fr` ;
  - Activer la configuration automatique pour les applications locales à `oui`.
- onglet `Certificats ssl` uniquement en mode expert :
  - Nom DNS/IP alternatif du serveur : `etab.ac-acad.fr` *(ré-générer les certificats si nécessaire)*.

Voir aussi...

Onglet Firewall [p.38]

Onglet Reverse proxy : Configuration du proxy inverse [p.82]

Onglet Eole sso : Configuration du service SSO pour l'authentification unique [p.66]

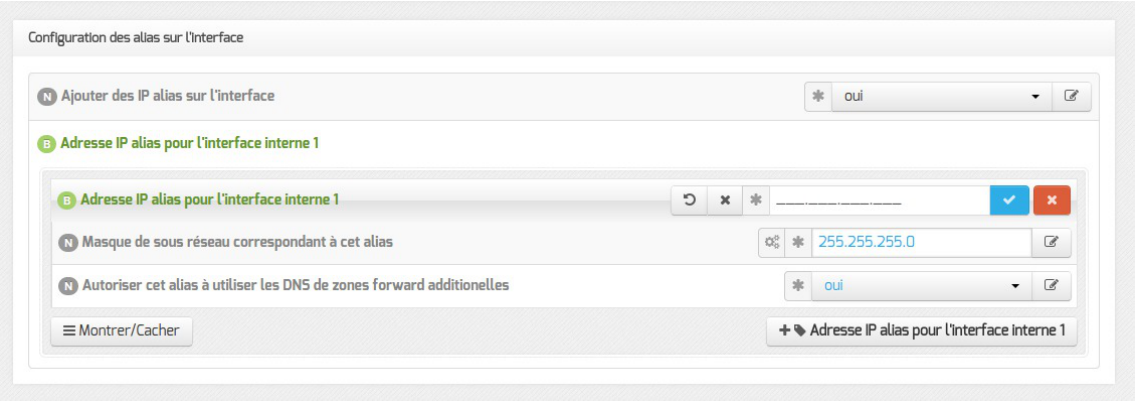
ERA, éditeur de règles pour le module Amon [p.235]

6. Configuration DNS pour chaque interface

Configuration des alias sur l'interface

Il est possible d'ajuster les paramètres du serveur DNS pour chaque alias sauf pour l'interface 0. Dans l'onglet des interfaces concernées `Interface-n` il faut dans la section `Configuration des alias sur l'interface` passer `Ajouter des IP alias sur l'interface` à `oui` et saisir :

- l'adresse IP alias ;
- le masque de sous réseau.



La variable `Autoriser cet alias à utiliser les DNS de zones forward additionnelles` permet d'autoriser le réseau de l'alias à résoudre les noms d'hôte des domaines déclarés dans la section `Forward de zone DNS` de l'onglet `Zones-dns`.

RVP

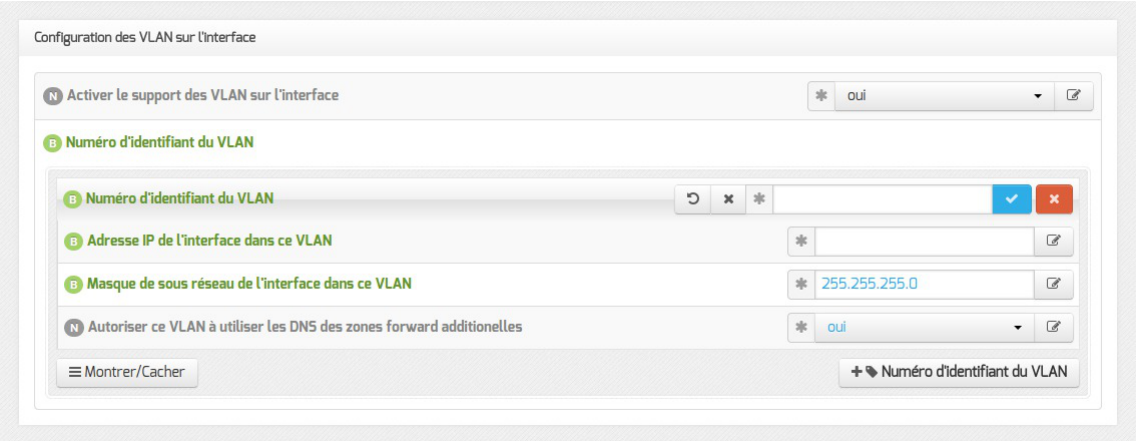
Si le service RVP est activé dans l'onglet `Services` et que le serveur est membre du réseau AGRIATES (`Serveur membre du réseau AGRIATES` à `oui` dans l'onglet `Rvp`) la variable `Autoriser cet alias à utiliser les DNS de forward RVP/AGRIATES` est disponible pour autoriser ou non le réseau de l'alias à résoudre les noms d'hôte de la zone AGRIATES.

Il est possible d'ajouter d'autres adresses IP alias sur l'interface en cliquant sur le bouton `+ Adresse IP alias pour l'interface n`.

Configuration des VLAN sur l'interface

Il est possible d'ajuster les paramètres du serveur DNS pour chaque VLAN sauf pour ceux de l'interface 0. Dans l'onglet des interfaces concernées `Interface-n` il faut dans la section `Configuration des VLAN sur l'interface` passer `Activer le support des VLAN sur l'interface` à `oui` et saisir :

- le numéro du VLAN ;
- l'adresse IP de l'interface dans ce VLAN ;
- le masque de sous réseau de l'interface dans ce VLAN.



La variable `Autoriser ce VLAN à utiliser les DNS de zones forward additionnelles` permet d'autoriser le réseau du VLAN à résoudre les noms d'hôte des domaines déclarés dans la section `Forward de zone DNS` de l'onglet `Zones-dns`.

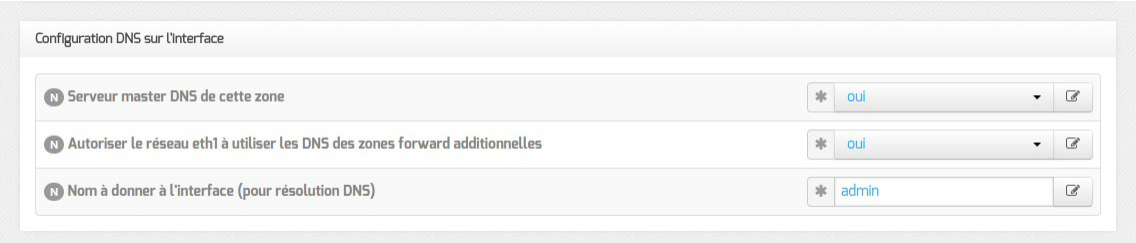
RVP

Si le service RVP est activé dans l'onglet `Services` et que le serveur est membre du réseau AGRIATES (`Serveur membre du réseau AGRIATES` à `oui` dans l'onglet `Rvp`) la variable `Autoriser ce VLAN à utiliser les DNS de forward RVP/AGRIATES` est disponible et permet d'autoriser ou non le réseau du VLAN à résoudre les noms d'hôte de la zone AGRIATES.

Il est possible d'ajouter d'autres VLAN sur l'interface en cliquant sur le bouton `+ Numéro d'identifiant du VLAN`.

Configuration DNS sur l'interface

Il est possible d'ajuster les paramètres du serveur DNS pour chaque interface sauf pour l'interface 0. Dans l'onglet des interfaces concernées `Interface-n` il faut adapter les paramètres de la section `Configuration DNS sur l'interface`.



- `Serveur master DNS de cette zone` : sert à activer le DNS sur l'interface.
- `Autoriser le réseau ethX à utiliser les DNS des zones forward additionnels` : permet d'autoriser le réseau ethX à résoudre les noms d'hôte des domaines déclarés dans la section `Forward de zone DNS` de l'onglet `Zones-dns`.
- `Nom à donner à l'interface (pour résolution DNS)` : entrée DNS correspondant à l'adresse IP de l'interface ethX. Le nom par défaut (admin pour l'interface eth1) est différent et doit rester pour chaque interface.

RVP

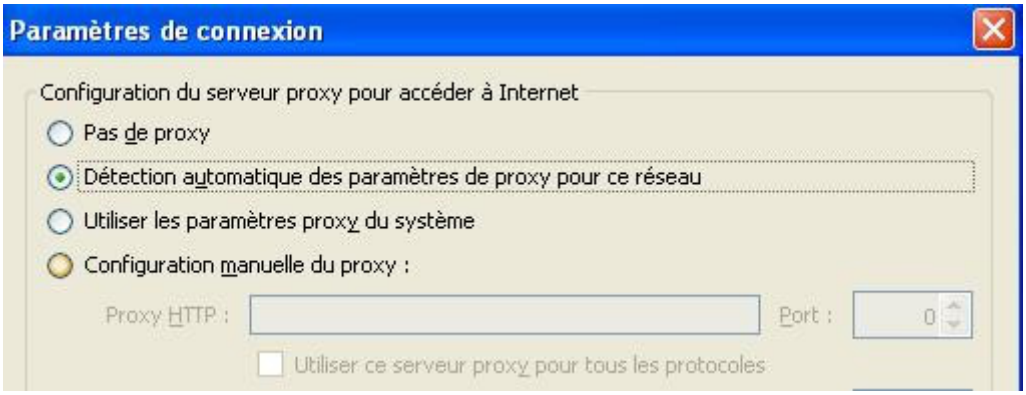
Si le service RVP est activé dans l'onglet `Services` et que le serveur est membre du réseau AGRIATES (`Serveur membre du réseau AGRIATES` à `oui` dans l'onglet `Rvp`) la variable `Autoriser le réseau ethX à utiliser les DNS de forward RVP/AGRIATES` est disponible et permet d'autoriser ou non le réseau ethX à résoudre les noms d'hôte de la zone AGRIATES.

7. Configurer la découverte automatique du proxy avec WPAD

WPAD[p.314] est un protocole qui permet la découverte automatique du proxy par les navigateurs.

Le principe est simple, si le navigateur est configuré pour détecter automatiquement la configuration du proxy, il essayera de télécharger le fichier : `wpad.<domaine_local>/wpad.dat` ou le fichier `proxy.pac`.

Configuration côté client



Détection automatique du proxy dans Firefox

Par défaut, les adresses pour lesquelles le proxy ne sera pas utilisé sont : 127.0.0.1 et le réseau local.

La détection automatique du proxy par les navigateurs peut être imposée par des outils tels que :

- ESU/client Scribe ;
- Gaspacho.

Dans le cas de l'activation du proxy Cntlm[p.303] le numéro de port change mais sa prise en charge est automatisée, il n'y a donc rien à faire.

Configuration côté serveur

Pour fonctionner correctement, WPAD a besoin de trois éléments qui sont pris en charge par EOLE :

- un serveur web qui diffuse le fichier, dans le cadre d'EOLE, c'est le service Nginx[p.308] qui se charge de distribuer les fichiers `wpad.dat` adaptés à chacun des sous-réseaux.
- un nom de domaine `wpad.<nom_domain_local>` qui pointe vers le serveur web ;

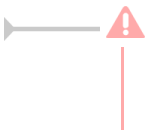
- un serveur DHCP configuré pour envoyer le chemin du fichier.

Par défaut, la configuration est correctement définie sur un AmonEcole mais dans le cadre d'un environnement Amon / Scribe ou Amon / Horus il faut configurer correctement les deux modules.

Configuration sur le module Scribe

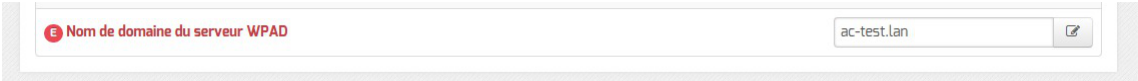
Le serveur DHCP doit être activé et correctement configuré sur le module Scribe.

Dans l'interface de configuration du module en mode expert, dans l'onglet `Dhcp`, le champ `Nom de domaine du serveur WPAD` permet de configurer le nom de domaine du serveur WPAD.



Même s'il est possible d'utiliser n'importe quel domaine, il est conseillé d'utiliser la même valeur que celle utilisée pour le nom de domaine local.

Pour les postes de travail Windows c'est la valeur du champ `Nom de domaine du serveur WPAD` qui sera utiliser pour accéder au fichier WPAD tandis que pour des postes de travail GNU/Linux c'est le nom de domaine local qui sera utilisé pour accéder au fichier WPAD.



Vue de l'onglet Dhcp de l'interface de configuration du module

Dans l'interface de configuration du module, en mode expert, il faut saisir dans le `Nom de domaine du serveur WPAD` de l'onglet `Dhcp` la même valeur que celle du champ `Nom de domaine privé du réseau local` de l'onglet `Général`.

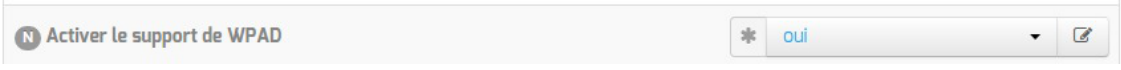
Pour être pris en compte, les changements doivent être enregistrés et suivis de la commande `reconfigure` sur le module.

Configuration sur le module Amon

WPAD est mise à disposition sur les modules Amon et ses variantes (AmonEcole, ...) au travers du paquet `eole-wpad` mais n'est fonctionnel que si le paquet `eole-proxy` est installé.

Pour fonctionner correctement, il faut que l'URL `wpad.<nom_domaine_local>` correspondre à l'adresse IP du serveur web.

Le support de WPAD doit être activé et correctement configuré sur le module Amon.



Activation de WPAD dans l'onglet Services

Dans l'onglet `Services` de l'interface de configuration du module `Activer le support de WPAD` doit être placé à `oui`.

Vue de l'onglet Wpad dans l'interface de configuration du module

Cela rend disponible l'onglet `Wpad` au sein duquel le `Nom de domaine du service WPAD` doit être rempli avec la même valeur que le `Nom de domaine privé du réseau local` présent dans l'onglet `Général`.

Si vous souhaitez utiliser un autre nom de domaine qui ne correspondrait pas au `Nom de domaine privé du réseau local` de l'onglet `Général`, il faut le déclarer dans le champ `Nom domaine local supplémentaire ou rien` de l'onglet `Zones-dns`.

Pour être pris en compte, les changements doivent être enregistrés et suivis de la commande `reconfigure` sur le module.

WPAD supporte les VLAN et les alias, Nginx renvoie le bon fichier WPAD si des VLAN ou des alias sont déclarés.

En mode expert, Il est également possible de changer le port du proxy diffusé par défaut pour une interface, un VLAN ou un alias donné.

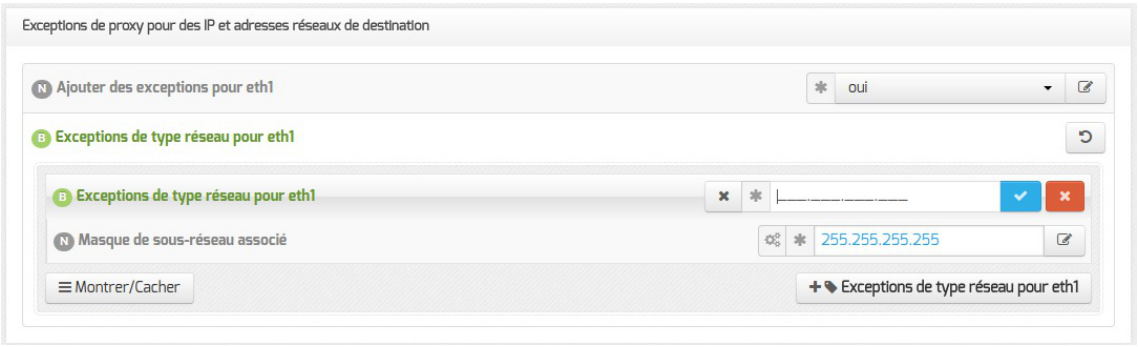
Ajouter des exclusions dans la configuration automatique du proxy

Dans l'onglet `Exceptions proxy` de l'interface de configuration du module il est possible d'ajouter des exclusions dans la configuration automatique du proxy.

Il est possible de déclarer différents types d'exceptions.

Exception sur une adresse IP ou une plage d'adresses IP

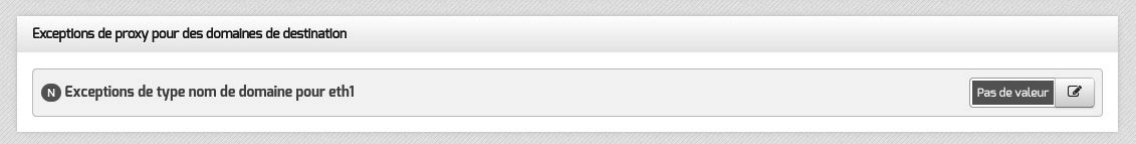
Cette exception commune à ERA et à WPAD permet de déclarer une adresse IP ou une plage d'adresses IP de destination pour laquelle on ne passe pas par le proxy.



Le bouton `Exceptions de type réseau pour eth-n` permet d'ajouter plusieurs exceptions sur une même interface.

Exception sur un nom de domaine

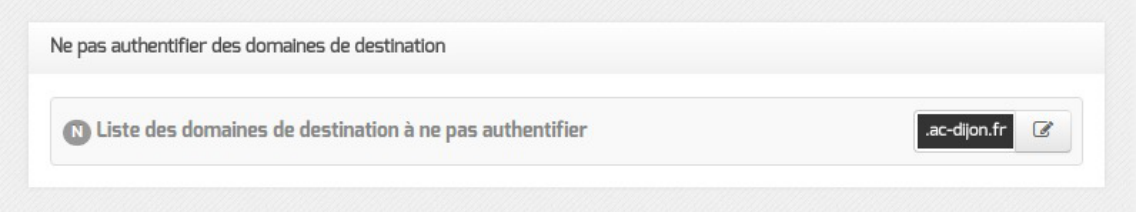
Cette exception commune à ERA et à WPAD permet de déclarer un domaine de destination pour lequelle on ne passe pas par le proxy.



Il est possible d'ajouter plusieurs exceptions sur une même interface.

Exception au niveau de l'authentification des domaines

Cette exception permet de déclarer des sites pour lesquels le proxy ne demandera pas l'authentification à l'utilisateur qui souhaite y accéder.



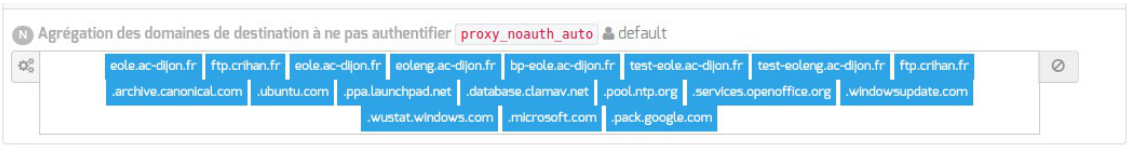
Si cNTLM et WPAD sur activés sur l'interface réseau, les utilisateurs utiliseront directement Squid (sans passer par cNTLM) pour accéder à ces sites.

Les domaines commençants par un `.` sont gérés, le domaine lui-même et les sous-domaines ne sont pas authentifiés.

Si on spécifie la valeur `.ac-dijon.fr` alors `ac-dijon.fr` et `www.ac-dijon.fr` seront autorisés sans authentification.

Une liste de sites à ne pas authentifier par défaut est stockée dans la variable cachée `proxy_noauth_auto`.

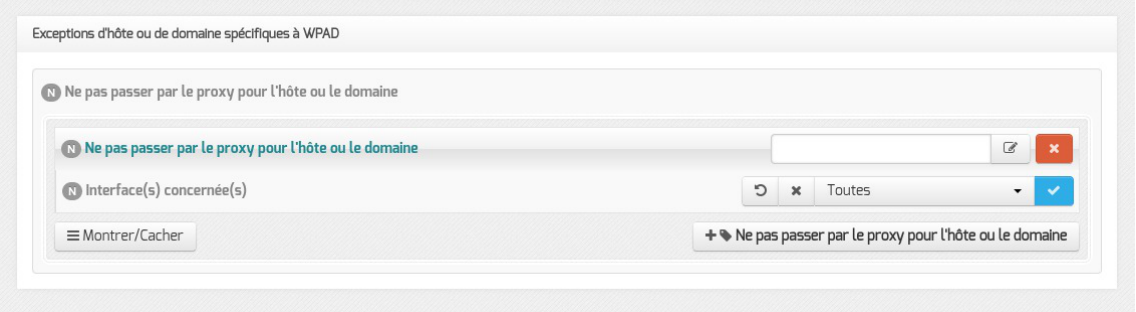
Il est possible de l'afficher dans l'onglet `Exceptions proxy` de l'interface de configuration du module en activant le mode Debug.



Cette variable reprend la liste des sites qui étaient dans le template `domaines_noauth` des versions EOLE antérieures à 2.5.2.

Exception sur un nom d'hôte (spécifique à WPAD)

L'exception sur un nom d'hôte s'effectue sur le nom d'hôte et sur le nom d'hôte complet.



Il faut choisir une interface ou toutes les interfaces sur lesquelles l'exception sera appliquée. Le bouton `+ Ne pas passer par le proxy pour l'hôte ou le domaine` permet d'ajouter plusieurs exceptions sur une même interface.

Ce type d'exception étant spécifique à WPAD, il n'est pas prise en compte par les autres services gérant des exceptions au niveau du proxy.

Si le champ `Ne pas passer par le proxy pour l'hôte ou le domaine` a comme valeur `www.ac-monacad.fr`, le fichier WPAD.dat généré contiendra la ligne `|| localHostOrDomainIs(host, "www.ac-monacad.fr")` qui permet d'exclure simplement des URLs.

Compléments sur `Ne pas passer par le proxy pour le domaine` (dnsDomainIs) :

http://findproxyforurl.com/netscape-documentation/#dnsDomainIs

Compléments sur `Ne pas passer par le proxy pour l'hôte ou le domaine` (localHostOrDomainIs) :

http://findproxyforurl.com/netscape-documentation/#localHostOrDomainIs

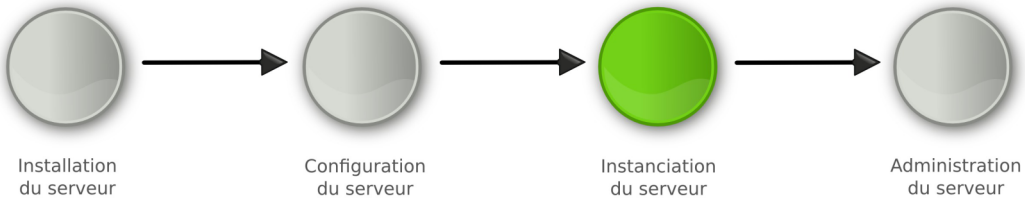
Configuration du serveur DHCP sur le module Scribe

Onglet Dhcp : Configuration du serveur DHCP

Chapitre 5

Instanciation du module

La troisième des quatre phases



Instanciation

Les généralités sur l'instanciation commune aux différents modules **ne sont pas traitées** dans cette documentation, veuillez vous reporter à la documentation de mise en œuvre d'un module EOLE ou à la documentation complète du module concerné.

- La **phase d'instanciation** s'effectue au moyen de la commande `instance` .

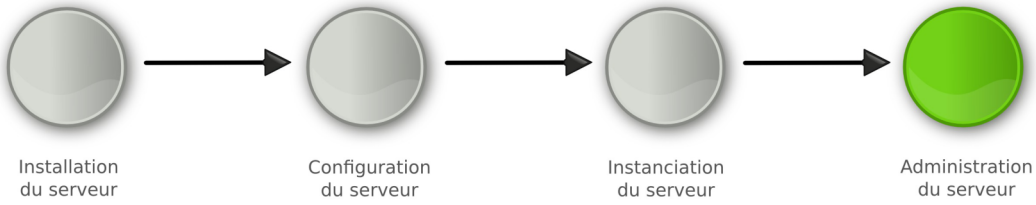
  L'instanciation permet de transférer les valeurs définies précédemment et des fichiers de configuration pré-remplis vers les fichiers cibles.

  À l'issue de cette phase, le serveur est utilisable en exploitation.

  Cette phase doit être complétée par un diagnostique complet du module à l'aide de la commande `diagnose -L` .

Chapitre 6

Administration du module Amon



Administration

Les généralités sur l'administration et l'administration commune aux différents modules ne sont pas traités dans cette documentation, veuillez vous reporter à la documentation de mise en œuvre d'un module EOLE ou à la documentation complète du module.

- La **phase d'administration** correspond à l'exploitation du serveur.
  Chaque module possède des fonctionnalités propres, souvent complémentaires.
  Diverses interfaces permettent la mise en œuvre de ces fonctionnalités et en facilitent l'usage.

1. Fonctionnalités de l'EAD propres au module Amon

1.1. Rôles et association de rôles

L'EAD est composé, comme nous l'avons vu précédemment, d'*actions*. Chaque action ayant un but bien précis.
L'EAD dispose d'un mécanisme de délégation d'*actions* à des utilisateurs bien déterminés.
Pour affecter certaines actions à un utilisateur, l'EAD utilise un mécanisme interne : les **rôles**.

Par défaut sur un module EOLE, l'utilisateur "*admin*" est associé au rôle "*administrateur*".

Plusieurs rôles sont prédéfinis sur les modules EOLE :

- administrateur ;
- professeur *(utilisé sur Scribe)* ;
- élève *(utilisé sur Scribe)* ;

- administrateur de classe *(utilisé sur Scribe)* ;
- administrateur du réseau pédagogique *(utilisé sur Amon)*.

1.1.1. Gestion des rôles

Les rôles de l'EAD sont déclarés dans les fichiers : `/usr/share/ead2/backend/config/perms/perm_*.ini`
Ces fichiers au format INI[p.306] permettent d'associer des actions (permissions) à un ou plusieurs rôles.

Fichiers pris en compte

Sur un module EOLE, seuls les fichiers suivants sont pris en compte :

- `/usr/share/ead2/backend/config/perm.ini` : rôles de base ;
- `/usr/share/ead2/backend/config/perm_<module>.ini` : rôles spécifiques au module installé (ex : `perm_scribe.ini`) ;
- `/usr/share/ead2/backend/config/perm_local.ini` : rôles déclarés localement (édition manuelle ou via l'EAD) ;
- `/usr/share/ead2/backend/config/perm_acad.ini` : rôles déclarés au niveau académique (via Zéphir) ;
- ainsi que tout les fichiers `perm_*.ini` présents dans le répertoire `/usr/share/ead2/backend/config/perms`.

Syntaxe des fichiers

Les permissions associent un rôle à une ou plusieurs actions.
Les fichiers `perm*.ini` doivent posséder une section `[role]` et une section `[permissions]`.

```
[role]
nom_du_role = libelle_du_role
[permissions]
action1 = nom_du_role
action2 = nom_du_role
```

Création de rôle via l'EAD

L'interface EAD permet de créer des rôles personnalisés.
Ces rôles ne sont, en fait, qu'une liste d'actions regroupées sous un intitulé et un libellé unique.
Il est possible, dans un deuxième temps d'associer ces rôles à des utilisateurs.

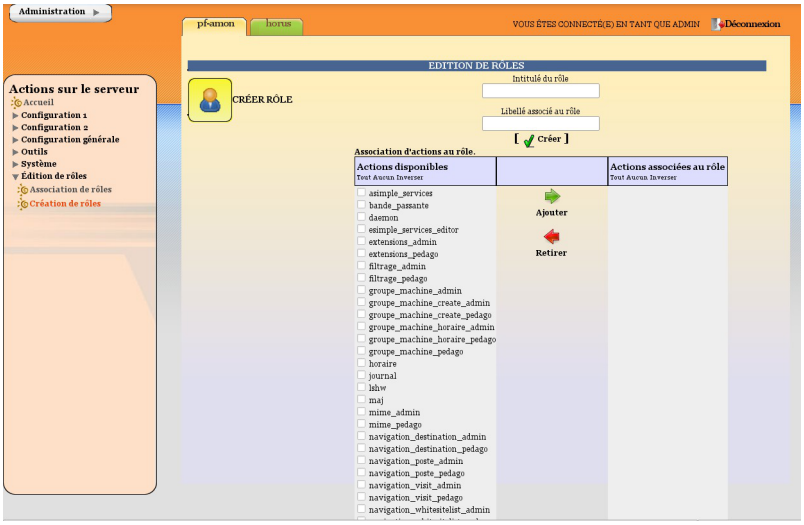
La fenêtre d'édition des rôles

Pour créer un nouveau rôle cliquer sur :

- Édition de rôles/Création de rôles

puis

- Créer rôle
- entrer l'intitulé (le nom) du rôle (sans caractère spécial, sans accent et sans espace) ;
- entrer un libellé (courte description) du rôle ;
- cocher les actions à autoriser ;
- ajouter ;
- créer.



Création d'un rôle

Actions obligatoires

Certaines actions doivent être obligatoirement permises pour tous les utilisateurs :

- **help** : utilisé notamment pour l'affichage d'aide ;
- **main_status** : page d'accueil appelée par défaut, elle gère un rôle prof (n'affiche pas les états de services) et un rôle admin ;
- **update_ead** : outil de téléchargement des javascripts, CSS, images spécifiques au module.

Actions communes aux différents modules

- **lshw** : listing matériel ;
- **maj** : action de mise à jour ;
- **daemon** : relancer des services (mode expert) ;

- **simple_services_editor** : éditer des groupes de services pour le mode simplifié ;
- **simple_services** : redémarrer/arrêter les services (mode simplifié) ;
- **server-configure**/**server-reboot**/**server-stop** : redémarrer/arrêter/reconfigurer le serveur ;
- **role_editor** : création de rôles ;
- **role_manager** : association de rôle (appelée par d'autres actions).

Actions spécifiques au module Amon

La modification du système de filtrage sur le module Amon apporte de profondes modifications sur ce module.

Selon les choix effectués lors de la phase de configuration avec l'interface de configuration du module, vous pouvez choisir d'utiliser une ou deux zones de configuration pour le filtrage et les options du pare-feu.

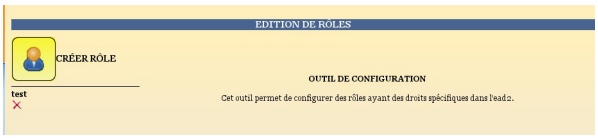
La zone 1 correspond à la réseau admin et la zone 2 correspond au réseau pedago.

- Gestion des postes
  - **navigation_poste_admin** (ou pedago) : action de gestion des postes à interdire ;
  - **navigation_destination_admin** (ou pedago) : interdire des destinations.
- Gestion des groupes de machine
  - **groupe_machine_admin** (ou pedago) : action d'entrée pour la gestion des groupes de machine (gère des restrictions pour le rôle prof) ;
  - **groupe_machine_create_admin** (ou pedago) : action de création de groupe de machine (nécessite groupe_machine) ;
  - **groupe_machine_horaire_admin** (ou pedago) : action de gestion des horaires pour les groupes de machine.
- Gestion des utilisateurs
  - **navigation_banned_user_admin** (ou pedago) : action de gestion des utilisateurs à interdire ;
  - **navigation_moderateur_admin** (ou pedago) : action de gestion des modérateurs ;
  - **navigation_whitelist_admin** (ou pedago) : action de gestion des utilisateurs en liste blanche ;
  - **navigation_whitesitelist_admin** (ou pedago) : action de gestion des sites en liste blanche.
- Gestion des sites
  - **opt_filters_admi**n (ou pedago) : gestion des filtres optionnels pour la zone de configuration 1 (ou 2) ;
  - **filtrage_admin** (ou pedago) : gestion du mode de filtrage syntaxique pour la zone de configuration 1 (ou 2) ;
  - **sites_interdits_admin** (ou pedago) : gestion des sites interdits pour la zone de configuration 1 (ou 2) ;
  - **sites_autorises_admin** (ou pedago) : gestion des sites autorisés pour la zone de configuration 1 (ou 2) ;
  - **extensions_admin** (ou pedago) : gestion des extensions interdites pour la zone de configuration 1 (ou 2) ;

  - **mime_admin** (ou pedago) : gestion des types mime interdits pour la zone de configuration 1 (ou 2).
- Gestion des règles du pare-feu
  - **regles** : mode de fonctionnement du pare-feu ;
  - **peertopeer** : autorisation/interdiction du peer to peer ;
  - **horaire** : horaire de fonctionnement du pare-feu.
- Autres actions
  - **navigation_visit** : action de consultation des logs ;
  - **filtrage_bayes** : action d'évaluation d'URL à l'aide du filtrage bayésien ;
  - **bande_passante** : outil de test de bande passante.

Modification et suppression de rôle via l'EAD

- Pour modifier un rôle, il suffit de cliquer sur le nom voulu ;
- pour le supprimer, cliquer sur la croix rouge associée.



Modification/suppression d'un rôle

1.1.2. Association des rôles

Les associations de rôle de l'EAD sont déclarées dans les fichiers : `/usr/share/ead2/backend/config/roles/roles_*.ini`
Ces fichiers au format INI[p.306] permettent d'associer des rôles à un ou plusieurs utilisateurs.

Fichiers pris en compte

Sur un module EOLE, seuls les fichiers suivants sont pris en compte :

- `/usr/share/ead2/backend/config/roles.ini` : associations de base (admin, eleve, prof, ...) ;
- `/usr/share/ead2/backend/config/roles_<module>.ini` : associations spécifiques au module installé (ex : `roles_scribe.ini`) ;
- `/usr/share/ead2/backend/config/roles_local.ini` : associations déclarés localement (édition manuelle ou via l'EAD) ;
- `/usr/share/ead2/backend/config/roles_acad.ini` : associations déclarés au niveau académique (via Zéphir).

Syntaxe des fichiers

L'association d'un rôle se fait à partir du login d'un utilisateur système (section `[pam]`) ou de la valeur associée à un attribut ldap (section `[nom attribut]`) de l'annuaire utilisé pour l'authentification SSO sur l'EAD du module.

```
[pam]
scribe2=admin
[uid]
 jean.dupont=prof admin
[user_groups]
minedu=admin_horus
```

La clé spéciale `[user_groups]` permet d'attribuer un rôle à tous les membres d'un groupe déclaré dans l'annuaire LDAP.

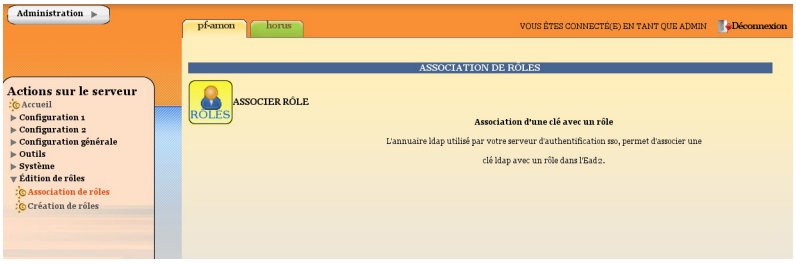
Création d'association via l'EAD

Quand un utilisateur se connecte sur l'EAD, en local ou en SSO, le système d'authentification renvoie des informations le concernant.

Certaines de ces informations sont utilisées pour lui attribuer des rôles et ainsi lui donner accès à certaines actions.

Pour associer un rôle à des utilisateurs:

- dans `Édition des rôles/Association de rôle` ;
- cliquer sur `Associer Rôle`.



La fenêtre d'association de rôles

- choisir la clef (attribut de l'utilisateur) ;
- renseigner la valeur recherchée pour cet attribut (dans le cas d'une authentification locale on mettra le login de l'utilisateur) ;
- choisir le rôle à associer ;
- valider.

Association d'un rôle

L'intitulé de la clef dépend du système d'authentification utilisé pour se connecter :

Authentification locale :

- le login de l'utilisateur.

Authentification SSO :

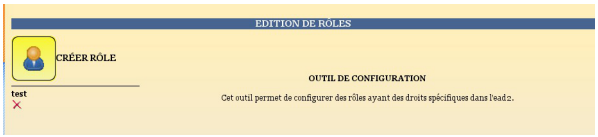
- l'élève fait partie de la classe ;

- la valeur de la clé LDAP typeadmin :
  - 0 → enseignant
  - 1 → administrateur
  - 2 → enseignant responsable de classe
  - 3 → personnel administratif
- le login de l'utilisateur ;
- le ou les groupes de l'utilisateur.

Il est indispensable de redémarrer le service ead-server dans `Système->Services (mode expert)` pour que les modifications soient prises en compte.

Suppression d'une association via l'EAD

Une association de rôle peut par la suite être supprimée en cliquant sur la croix rouge.



Modification/suppression d'un rôle

1.1.3. Les rôles sur le module Amon

L'EAD est accessible aux utilisateurs *root* et *eole* (authentification locale), *admin* et à tous les *professeurs* (authentification SSO).

En fonction de l'utilisateur un rôle différent peut être appliqué. À chaque rôle est affecté différentes actions.

Il existe, par défaut, 3 rôles dans l'EAD :

- administrateur : accès à toutes les actions (ex. redémarrage des services, mise à jour du serveur, création et affectation des rôle aux autres utilisateurs, etc.) ;
- administrateur du serveur Amon (utilisé sur le module Amon) ;
- administrateur du réseau pédagogique (utilisé sur le module Amon).

Il est possible de créer davantage de rôles ayant accès à diverses actions afin, par exemple, de donner le droit à un professeur de pouvoir redémarrer un groupe de services en plus de ses autorisations de base.

Accès "administrateur"

Par défaut, les utilisateurs *admin*, *root* et *eole* ont accès à toutes les fonctions.

L'accès avec les utilisateurs *root* et *eole* s'effectue en utilisant l'authentification locale.

L'EAD, dans son mode le plus complet, présente les fonctions suivantes :

- distribution de devoirs ;
- création/gestion des utilisateurs, des groupes et des partages ;

- configuration et gestion des imprimantes (CUPS) ;
- importation CSV/Sconet/AAF/BE1D ;
- gestion des quotas ;
- observation des virus ;
- gestion des listes de diffusion ;
- modification du mode de contrôle des élèves ;
- consultation de l'historique des connexions ;
- envoi d'un message aux utilisateurs connectés ;
- extinction/redémarrage/fermeture de session sur les postes clients ;
- gestion des comptes de machine ;
- paramétrage et programmation des sauvegardes du serveur ;
- redémarrage des services ;
- mise à jour ;
- arrêt/redémarrage du serveur.

Accès "administrateur de l'Amon"

Cette partie n'est pas encore documentée #fixme

Accès "administrateur du réseau pédagogique"

Cette partie n'est pas encore documentée #fixme

1.2. Directives optionnelles ERA depuis l'EAD

Les modèles de pare-feu ERA peuvent contenir des directives optionnelles[p.304].

Une règle peut être :

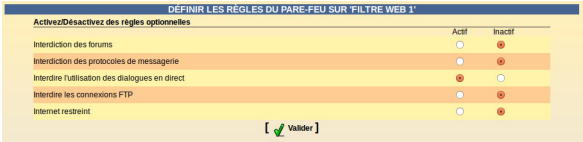
- générale, si elle concerne l'interface externe ;
- spécifique à une zone de configuration, si elle concerne une interface interne de la zone.

La configuration générale est accessible par le menu EAD : `Configuration générale` / `Règles du pare-feu`.

La configuration spécifique est accessible par le menu EAD : `Filtre web X` / `Règles du pare-feu` :

Pour valider une directive optionnelle :

- choisir Actif ;
- valider.



L'interface graphique d'ERA

Lien entre ERA et les directives optionnelles de l'EAD

Pour les règles optionnelles, l'EAD prime sur l'ERA : elles sont pilotées par l'EAD. Une directive peut être marquée comme étant active par défaut dans ERA et ne pas être active car désactivée dans l'interface EAD.

Voir aussi...

Les directives optionnelles [p.255]

1.3. Exceptions sur la source ou la destination

Par défaut, tous les accès à des sites nécessitent une authentification (si elle est active) et toutes les machines du réseau doivent s'identifier. Mais certains systèmes ou logiciels doivent pouvoir se mettre à jour de façon transparente.

Par ailleurs, le proxy conserve une version des pages téléchargées en cache pour limiter la consommation réseau. Ce comportement n'est pas adapté à tous les sites.

Pour les sites comportant des données sensibles, il est nécessaire de s'assurer que des données relatives à la navigation sur ce domaine ne soient pas placées dans le cache du serveur.

Certaines machines peuvent également avoir besoin de naviguer avec des données provenant directement du site consulté.

Certains postes clients ou serveurs du réseau ont besoin d'effectuer des mises à jour automatiquement, les sites de mise à jour doivent être accessibles sans authentification.

Certaines machines peuvent également avoir besoin de naviguer sans être authentifiées.

Pour cela, il existe deux mécanismes :

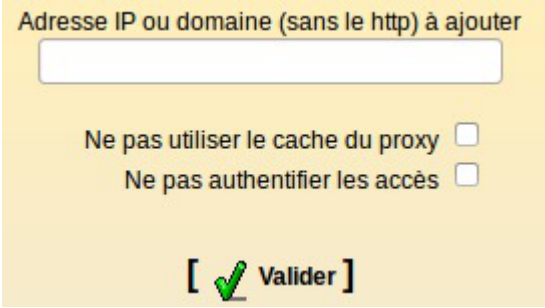
- ne pas utiliser de cache ou d'authentification pour certains sites (destination) ;
- ne pas utiliser de cache ou d'authentification pour certaines machines locales (source).

Pour paramétrer les destinations et les sources qui n'utiliseront pas le cache ou l'authentification lors de la navigation il faut se rendre dans `Configuration générale` puis `Cache et Authentification` de l'interface EAD du module.

Cache et authentification de la destination

Dans `Configuration générale` / `Cache et Authentification` / `Destinations` :

- entrer l'adresse IP ou le nom du domaine ;
- cocher authentification et/ou cache ;
- valider.



Ajout d'une destination à ne pas authentifier et/ou pour laquelle ne pas utiliser le cache

Pour supprimer une référence, cliquer sur la croix rouge correspondante :

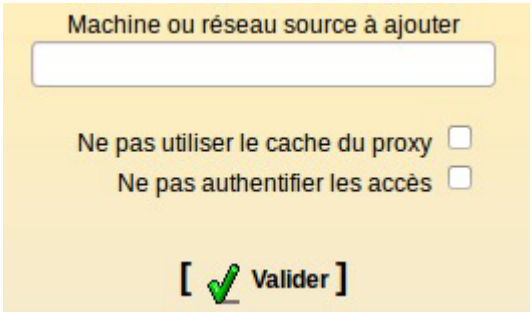
Destination	Cache	Authentification
10.121.58.5	✗	✗
ac-dijon.fr	✗	✗
scribe		✗

Listes des destinations à ne pas authentifier et/ou pour lesquelles ne pas utiliser le cache

Cache et authentification de la source

Dans `Configuration Générale` / `Cache et Authentification` / `Sources` :

- entrer l'adresse IP ou réseau
- cocher authentification et/ou cache ;
- valider.



Ajout d'une source à ne pas authentifier et/ou pour laquelle ne pas utiliser le cache

Pour supprimer une référence, cliquer sur la croix rouge correspondante :

Source	Cache	Authentification
10.121.58.5	✗	✗
10.21.58.10	✗	✗
172.16.0.0/24		✗
172.16.0.6	✗	✗

Listes des sources à ne pas authentifier et/ou pour lesquelles ne pas utiliser le cache

Personnalisations académiques

Des listes de sites et d'adresses académiques peuvent être gérées indépendamment de l'EAD par l'intermédiaire des fichiers suivants :

- `/etc/squid3/domaines_nocache_acad` : liste de destinations pour lesquelles ne pas utiliser le cache ;
- `/etc/squid3/src_noauth_acad` : liste de sources à ne pas authentifier ;

- `/etc/squid3/src_nocache_acad` : liste de sources pour lesquelles ne pas utiliser le cache ;
- `/etc/squid3/domaines_nopeerproxy` : liste de destinations pour lesquelles on n'utilise pas le proxy père.

L'utilisation du fichier `/etc/squid3/domaines_noauth_acad` pour gérer la liste de destinations à ne pas authentifier est dépréciée depuis la version 2.5.2. Il faut utiliser la fonctionnalité de l'onglet `Exceptions proxy` de l'interface de configuration du module.

Voir aussi...

Configurer la découverte automatique du proxy avec WPAD [p.197]

1.4. Filtrage web

Avec le filtrage web, il est possible :

- de configurer la manière dont le filtrage s'effectue ;
- d'associer une politique de filtrage (interdits, modérateurs, liste blanche...) à des utilisateurs (seulement si l'authentification est activée durant la phase de configuration) ;
- d'associer une politique de filtrage (interdits, modérateurs, liste blanche...) à des machines.

Cette configuration s'effectue :

- par zone de configuration ;
- de manière plus fine, par politique de filtrage ;
- de façon prioritaire sur les machines puis sur les utilisateurs.

1.4.1. Filtrage par utilisateur

Si l'authentification a été activée sur la zone durant la phase de configuration, il est possible de définir, pour l'utilisateur, une des politiques de filtrage suivante :

- modérateur (lorsqu'un site est interdit, un lien lui est proposé pour outrepasser l'interdiction) ;
- interdits (aucune navigation web n'est possible pour cet utilisateur) ;
- mode liste blanche (seuls les sites de la liste blanche sont autorisés) ;
- politique de filtrage web spécifique.

Placer un professeur sur la liste des modérateurs pour la zone de filtre web 1

Il est parfois intéressant de voir un site interdit, qui, parfois, empêche l'accès à un contenu pédagogique. En définissant un professeur comme modérateur, on lui permet d'outrepasser l'interdiction de navigation et, le cas échéant, le placer sur la liste des sites autorisés.

Dans `Filtre web 1` / `Utilisateurs` :

- entrer le nom de l'utilisateur ;

- valider ;
- choisir `Modérateur` dans la liste.

Configurer des politiques de filtrage pour un utilisateur sur la zone de filtre web 2

Ces informations sont stockées dans :

`/var/lib/blacklists/dansguardian<num_instance>/common/filtergroupslist`

Sur AmonEcole, ces fichiers sont dans le conteneur ***`reseau`***.

Si le menu `Utilisateurs` n'apparaît pas, c'est que la zone n'est pas authentifiée.

1.4.2. Filtrage par machine ou par groupe de machine

Présentation

Le module Amon propose de gérer des groupes de machine par plage d'adresse IP.

En ajoutant une référence à ce groupe, il est possible :

- de lui interdire l'accès au réseau ;
- de lui interdire la navigation web seulement ;
- de lui autoriser la navigation web selon des horaires ;
- de lui associer une politique de filtrage web spécifique.

Les informations liées aux groupes de machine sont stockées dans :

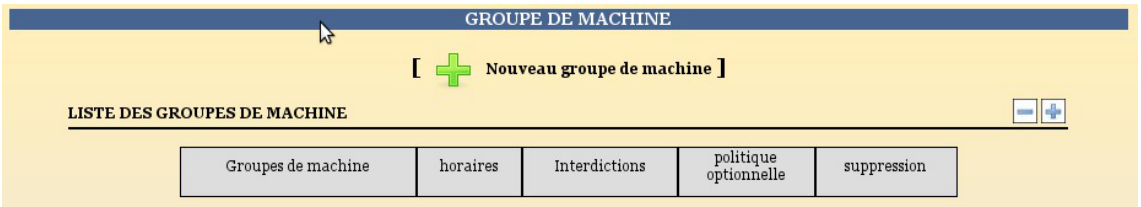
`/usr/share/ead2/backend/tmp/ipset_group<num_instance>.txt`

Les éventuelles plages horaires associées sont dans :

`/usr/share/ead2/backend/tmp/ipset_schedules<num_instance>.pickle`

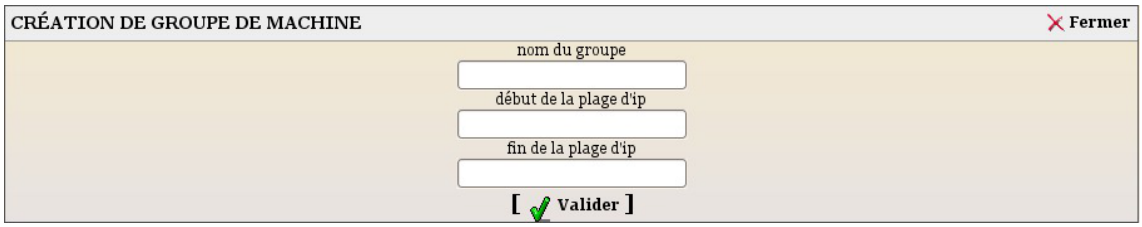
Créer un groupe de machine

Pour configurer un groupe de machine de la zone 1, aller dans `Filtre web 1` / `Groupe de machine`.



Interface de gestion de groupe de machine

Cliquer sur Nouveau groupe de machine et un formulaire de création apparaît.

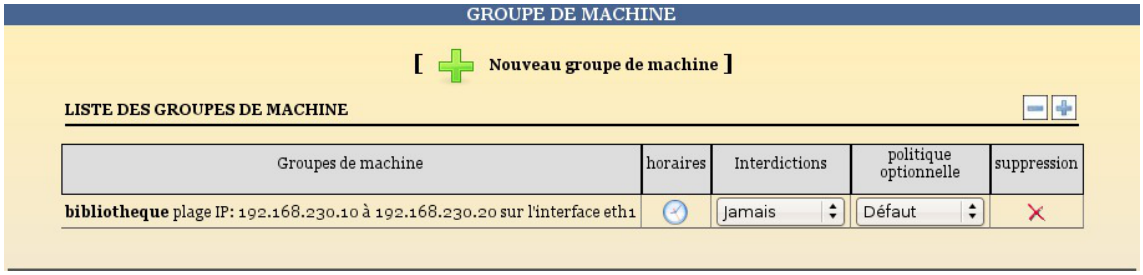


Formulaire de création

Remplir :

- nom pour le groupe de machine (sans accents ni caractères spéciaux) ;
- donner l'adresse IP de début de plage ;
- donner l'adresse IP de fin de plage ;
- si plusieurs interfaces réseau sont associés à cette zone, il vous demandera le nom de l'interface ;
- valider.

Le groupe de machine est dans la liste et peut être géré.



Le groupe de machine est ajouté

S'il ne vous est pas possible de choisir l'interface de votre groupe lors de sa création, c'est qu'une seule interface du pare-feu est associée à cette zone.

À partir de la version 2.5.2 d'EOLE, il n'est plus obligatoire que la plage d'adresse du groupe soit de classe C.

Un trop grand nombre d'adresses dans un groupe peut entraîner une baisse de performance.

Limiter l'accès réseau

Dans la colonne Interdictions, il est possible de choisir parmi :

- jamais ;
- le web tout le temps ;
- le web selon des horaires (à définir au préalable) ;
- toute activité réseau.

Interdire le groupe de navigation web

Dans la colonne Interdictions, choisir Le web tout le temps

Le groupe de machine est alors interdit d'accès sur les ports :

- 80 (HTTP)
- 443 (HTTPS)

- 3128 (e2guardian)
- 8080 (Squid)

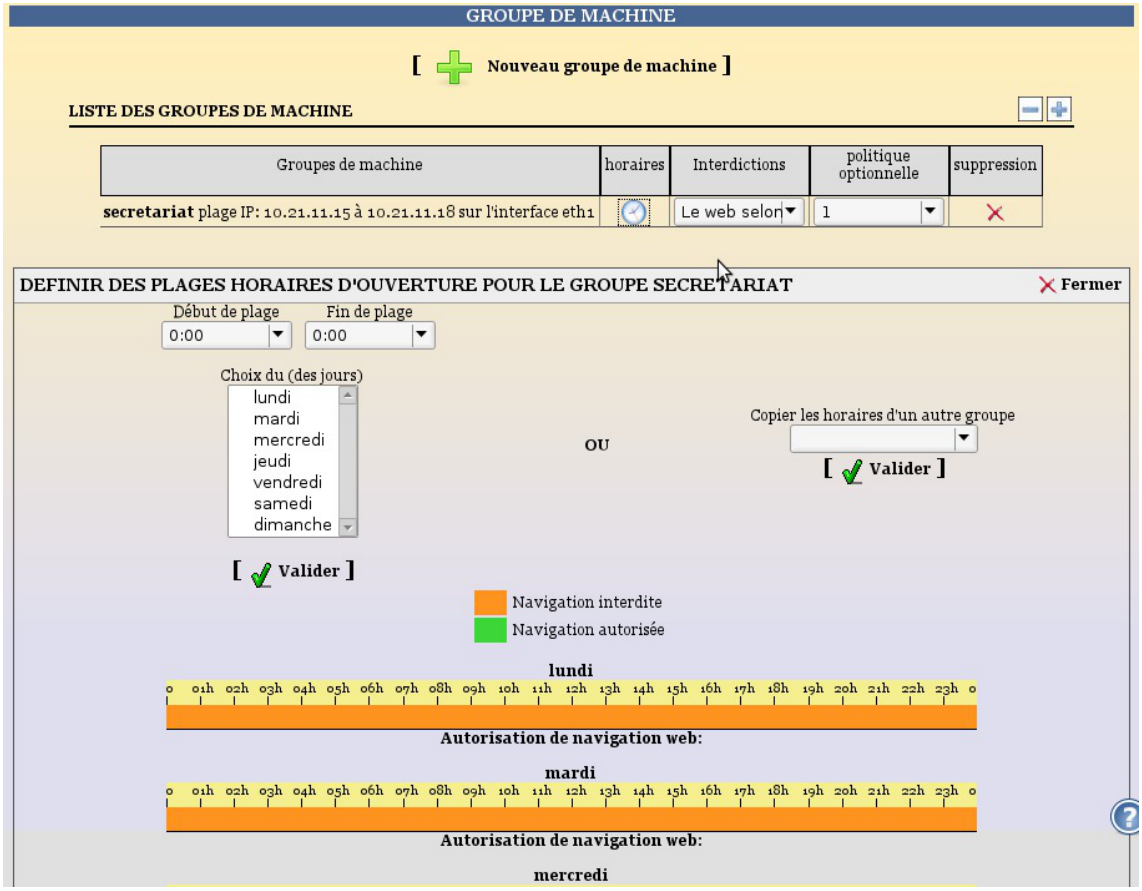
Si vous désirez faire une interdiction de navigation selon des horaires, il faut :

- configurer des horaires ;
- appliquer l'interdiction.

Configuration des horaires

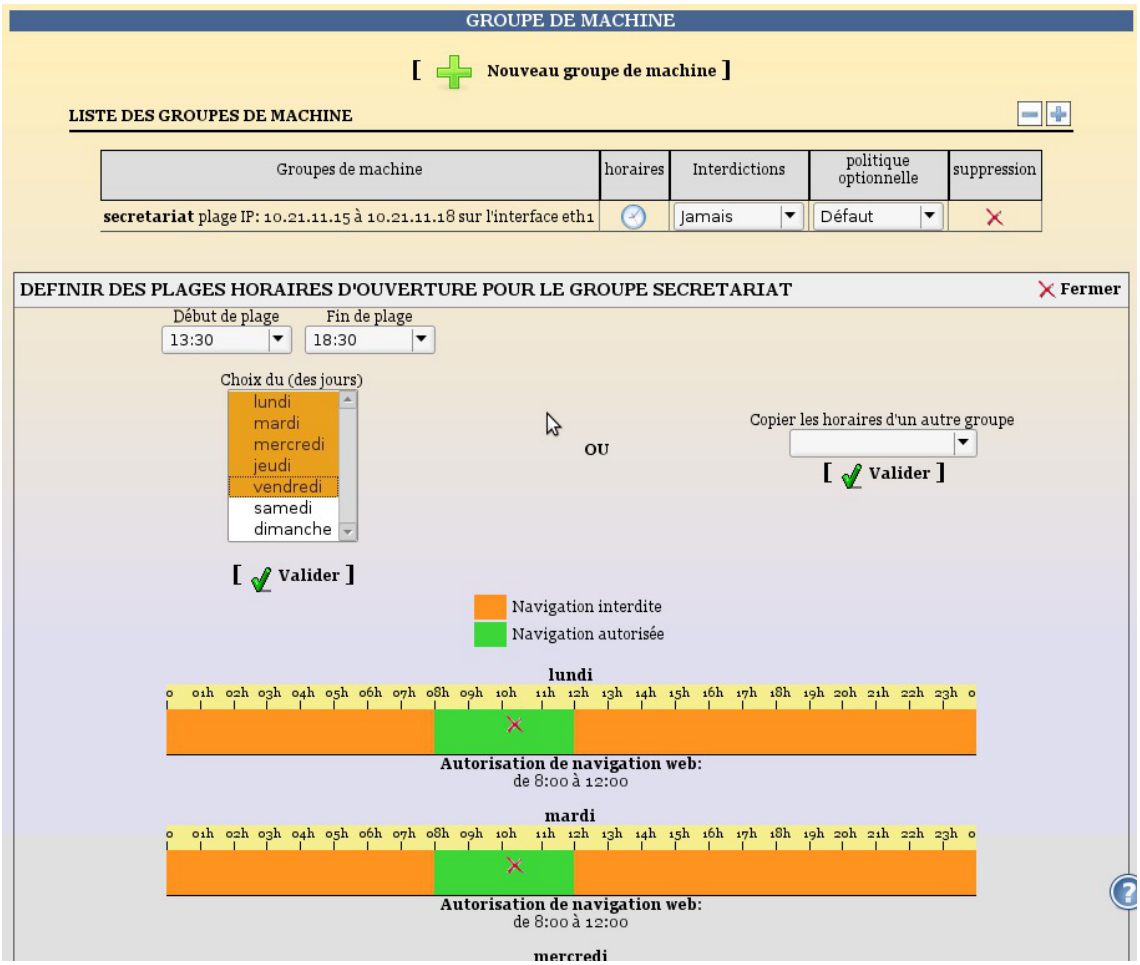
Dans la colonne `Interdictions`, choisir `Le web selon horaires`.

Cliquer sur l'horloge, la gestion des horaires apparaît.



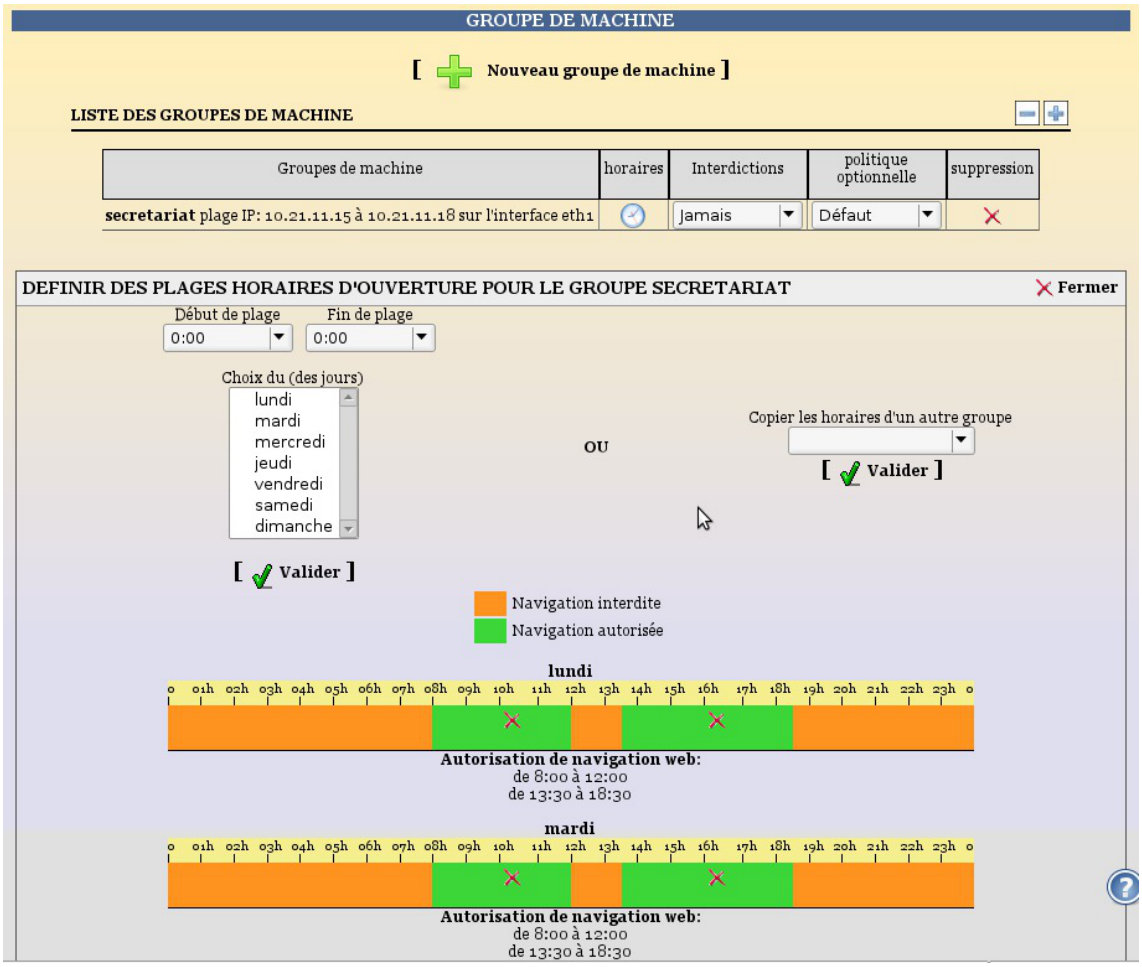
Gestionnaire d'horaires pour les groupes de machine

- choisir la plage horaire d'autorisation ;
- choisir les jours d'applications ;
- valider.



Remplir le formulaire

Les plages horaires définies s'affichent (la croix permet de supprimer la plage).



Affichage des plages horaires

Sans plage horaire définie, la navigation web est interdite tout le temps

La modification des plages horaires est dynamique.

Si le groupe de machine est interdit de navigation web selon horaires, il est possible de modifier les plages horaires.

Il est aussi possible de copier les horaires depuis un autre groupe de machine.

- choisir le groupe dans la liste ;
- valider.

Interdire l'accès au réseau

Pour interdire tout accès réseau à notre groupe de machine, dans la colonne `Interdictions`, choisir `Toute activité réseau`.

Spécifier une politique de filtrage

Il est possible d'associer une politique de filtrage au groupe de machine. Pour cela choisir la politique dans la colonne `politique optionnelle`.

Certaines politiques de filtrage sont fixes :

- modérateur ;
- interdit ;

- mode liste blanche.

D'autres sont configurables :

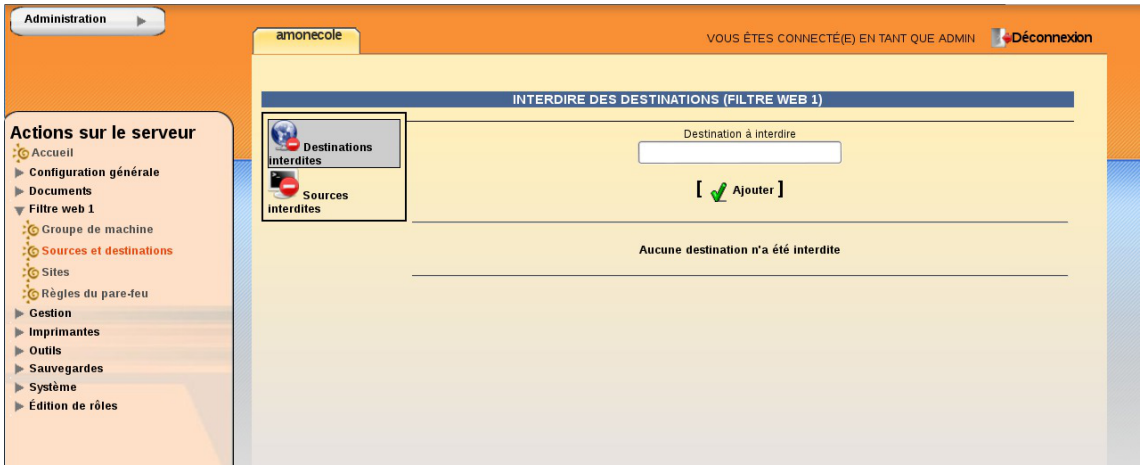
- Défaut ;
- 1 ;
- 2 ;
- 3 ;
- 4.

Supprimer un groupe de machine

Pour supprimer un groupe de machine, cliquez sur la croix en face de votre groupe de machine.

1.4.3. Interdire l'accès à un sous-réseau depuis une interface

Dans l'EAD il est possible d'interdire l'accès à un sous-réseau depuis une interface.



Vue d'ensemble pour l'ajout d'une destination à interdire

Dans le menu de l'EAD, choisir l'entrée portant le nom du filtre choisi dans l'interface de configuration du module, par défaut `Filtre web 1`. Puis sélectionner `Sources et destinations` et enfin `Destinations interdites`.

Pour interdire une destination il faut :

- définir le sous-réseau (ou le poste) de destination ;
- choisir l'interface source depuis laquelle interdire l'accès (n'apparaît que s'il existe plusieurs interfaces rattachées au filtre web sélectionné).

Nommage des filtres dans la configuration du filtrage web

> Configuration du filtrage web (cf. Onglet Filtrage web : Configuration du filtrage web) [p.157]

Interdire l'accès au sous-réseau 10.121.11.0/255.255.255.0 depuis l'interface admin (eth1)

Ajout d'une destination à interdire

Soit l'interface eth1 sur la zone de filtre web 1.

- Saisir `10.121.11.0/255.255.255.0` dans `Destinations à interdire` ;
- Choisir `admin (eth1)` dans la liste `Interface associée à l'adresse` ;
- Cliquer sur `Ajouter`.

Un message de confirmation "L'adresse 10.121.11.0/255.255.255.0 a été ajoutée à la liste des destinations interdites. Le pare-feu a bien été redémarré" apparaît.

Annuler une interdiction

Dans le menu de l'EAD, choisir l'entrée portant le nom du filtre choisi dans l'interface de configuration du module, par défaut `Filtre web 1`. Puis sélectionner `Sources et destinations` et enfin `Destinations interdites`.

Suppression d'une destination interdite

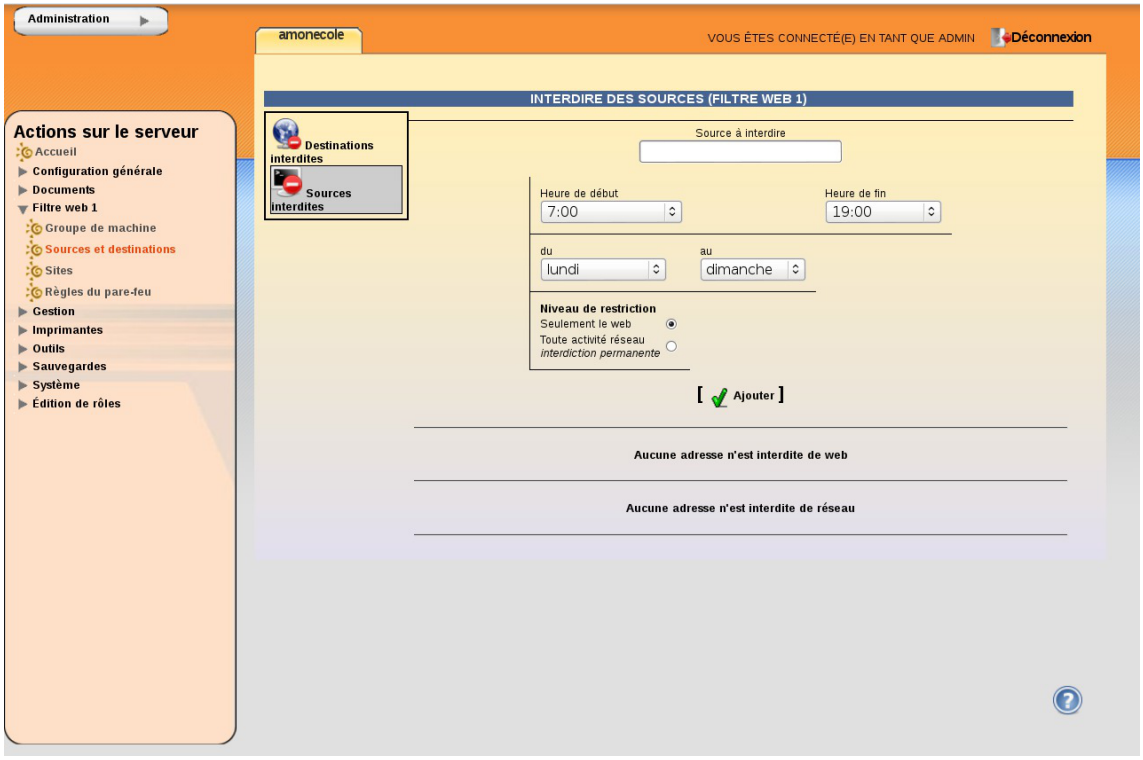
- Choisir l'interdiction à supprimer dans la liste ;
- Cliquer sur `Supprimer`.

Les destinations interdites sont écrites dans :

`/usr/share/ead2/backend/tmp/dest_interdites<num_instance>.txt`

1.4.4. Interdire ou restreindre l'activité d'un sous-réseau

Dans l'EAD il est possible d'interdire l'accès web en fonctions de plages horaires ou d'interdire l'activité à tout un sous-réseau .



Vue d'ensemble pour l'ajout d'une source à interdire

Dans le menu de l'EAD, choisir l'entrée portant le nom du filtre choisi dans l'interface de configuration du module, par défaut `Filtre web 1`. Puis sélectionner `Sources et destinations` et enfin `Sources interdites`.

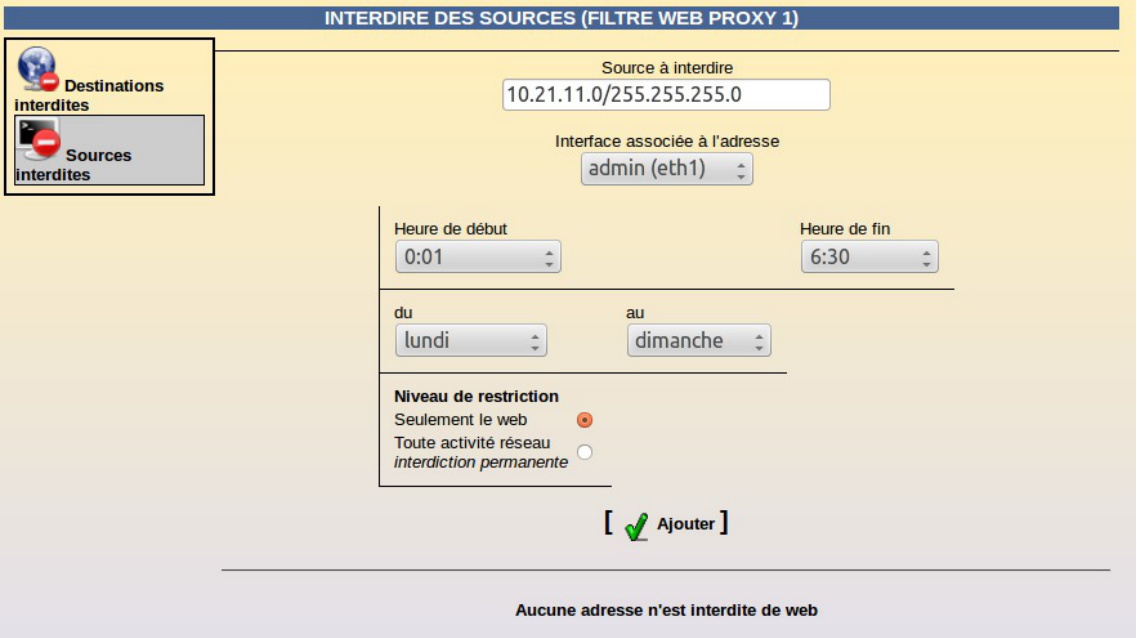
Les paramètres à saisir sont :

- la `Source à interdire` : le sous-réseau (ou poste) sur lequel les restrictions doivent être appliquées ;
- l'`Interface associée à l'adresse` (n'apparaît que s'il existe plusieurs interfaces rattachées au filtre web sélectionné) ;
- les plages horaires et journalières de la restriction (restriction web uniquement) ;
- le `Niveau de restriction` : web ou réseau.

Nommage des filtres dans la configuration du filtrage web

> Configuration du filtrage web (cf. Onglet Filtrage web : Configuration du filtrage web) [p.157]

Interdire l'accès web depuis le sous-réseau 10.21.11.0/255.255.255.0 provenant de l'interface eth1 tous les jours entre minuit et 6 heures du matin



Ajout d'une source à interdire

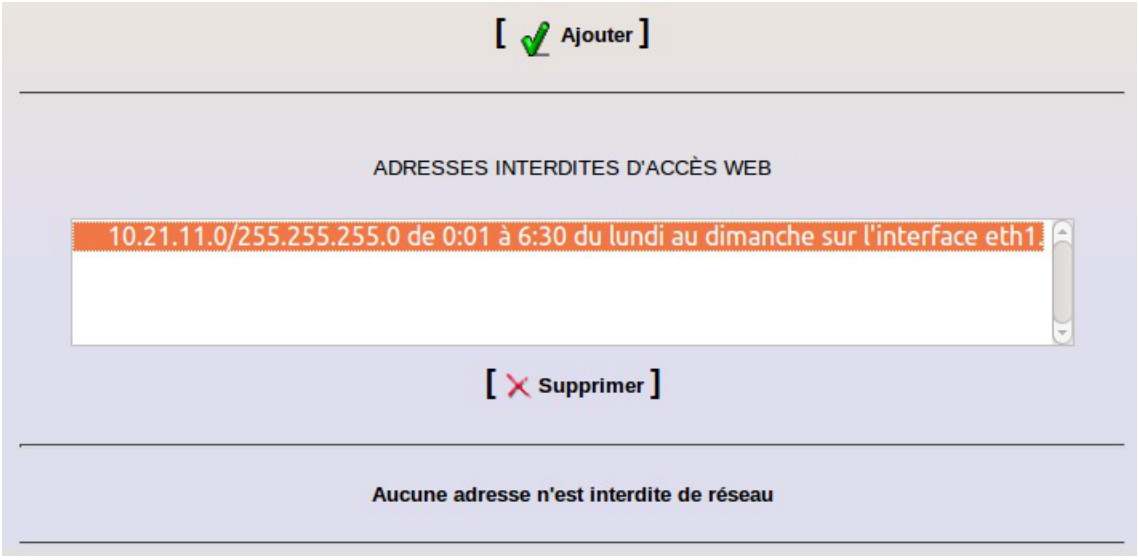
Soit l'interface eth1 sur la zone de filtre web 1 :

- Saisir `10.121.11.0/255.255.255.0` dans `Source à interdire` ;
- Choisir `admin (eth1)` dans la liste `Interface associée à l'adresse` ;
- Sélectionner `0:01` comme heure de début et `06:30` comme heure de fin ;
- Sélectionner les jours : du lundi au dimanche ;
- Choisir `Seulement le web` comme `Niveau de restriction` ;
- Cliquer sur `Ajouter`.

Un message de confirmation "L'adresse 10.121.11.0/255.255.255.0 a été ajoutée à la liste des postes interdits de navigation web. Le pare-feu a bien été redémarré" apparaît.

Annuler une interdiction

Dans le menu de l'EAD, choisir l'entrée portant le nom du filtre choisi dans l'interface de configuration du module, par défaut `Filtre web 1`. Puis sélectionner `Sources et destinations` et enfin `Sources interdites`.



Suppression d'une source interdite

- Choisir l'interdiction à supprimer dans la liste ;
- Cliquer sur Supprimer.

Les sources interdites d'accès web sont écrites dans :
/usr/share/ead2/backend/tmp/horaire_ip<num_instance>.txt
Les sources interdites d'accès réseau sont écrites dans :
/usr/share/ead2/backend/tmp/poste_all<num_instance>.txt

1.4.5. Bases de filtres optionnels

Les bases de filtres proposées sur le module Amon sont des copies de celles gérées par l'université de Toulouse 1 Capitole : http://cri.univ-tlse1.fr/blacklists [http://cri.univ-tlse1.fr/blacklists/] .

L'université de Toulouse 1 Capitole diffuse depuis de nombreuses années une liste noire d'URLs, gérée par Fabrice Prigent afin de permettre un meilleur contrôle de l'utilisation d'Internet.

Les bases, publiées sous licence d'utilisation Creative Commons by-sa 4.0 [http://creativecommons.org/licenses/by-sa/4.0/deed.fr] , sont largement utilisées par les écoles et sont également intégrées dans un grand nombre d'outils libres ou commerciaux, en complément d'autres listes.

Les bases sont mises à jour 2 à 3 fois par semaine en fonction des disponibilités du mainteneur, elles peuvent être enrichies grâce à une formulaire en anglais : http://dsi.ut-capitole.fr/cgi-bin/squidguard_modify.cgi.

Ces bases de filtres proposent des catégories avec des listes de domaines et d'URL triés par catégories.

Les sites référencés dans les catégories `adult` et `redirector` sont interdits d'office.

Les autres bases de filtres sont activables depuis l'interface EAD.

L'activation se fait :

- par filtre web ;
- par politique de filtrage.

La mise à jour des bases de filtres est lancée automatiquement toutes les nuits

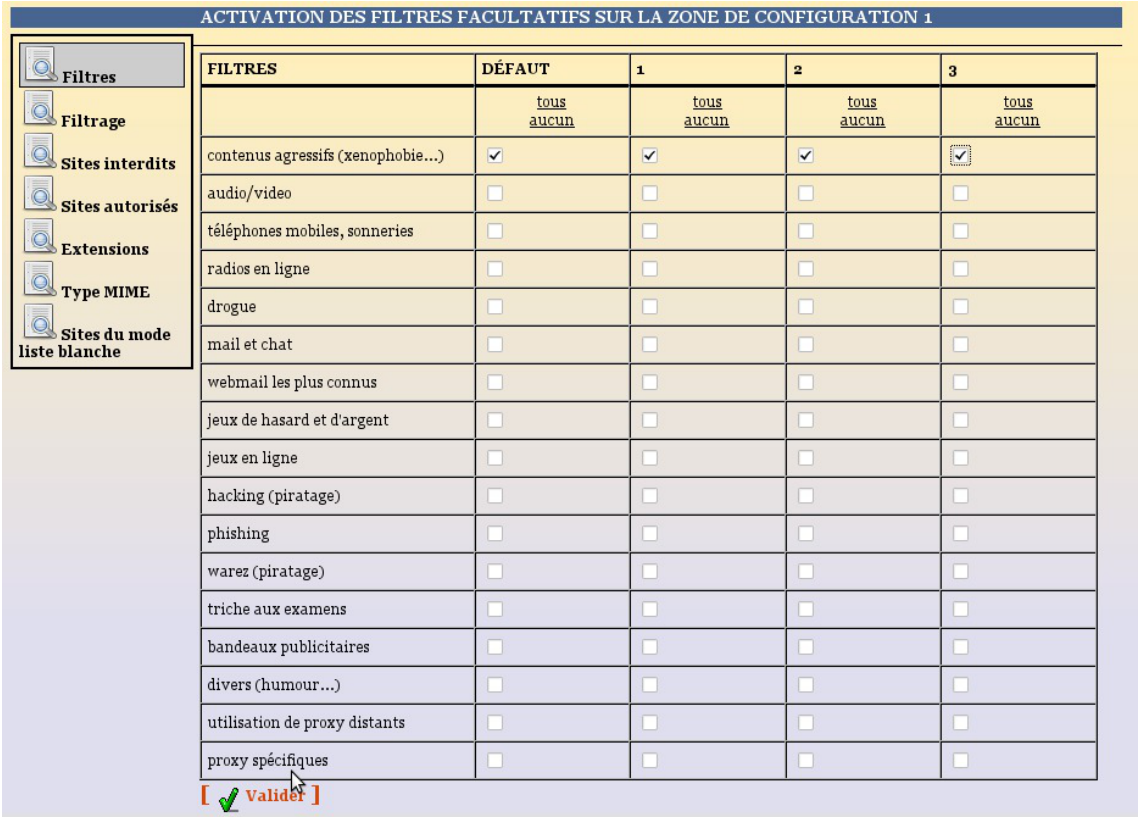
Un rapport de mise à jour est disponible sur la page d'accueil de l'EAD.

Rapport de mise à jour des bases de filtres

Pour activer la catégorie "agressif" sur toute la zone de configuration 1

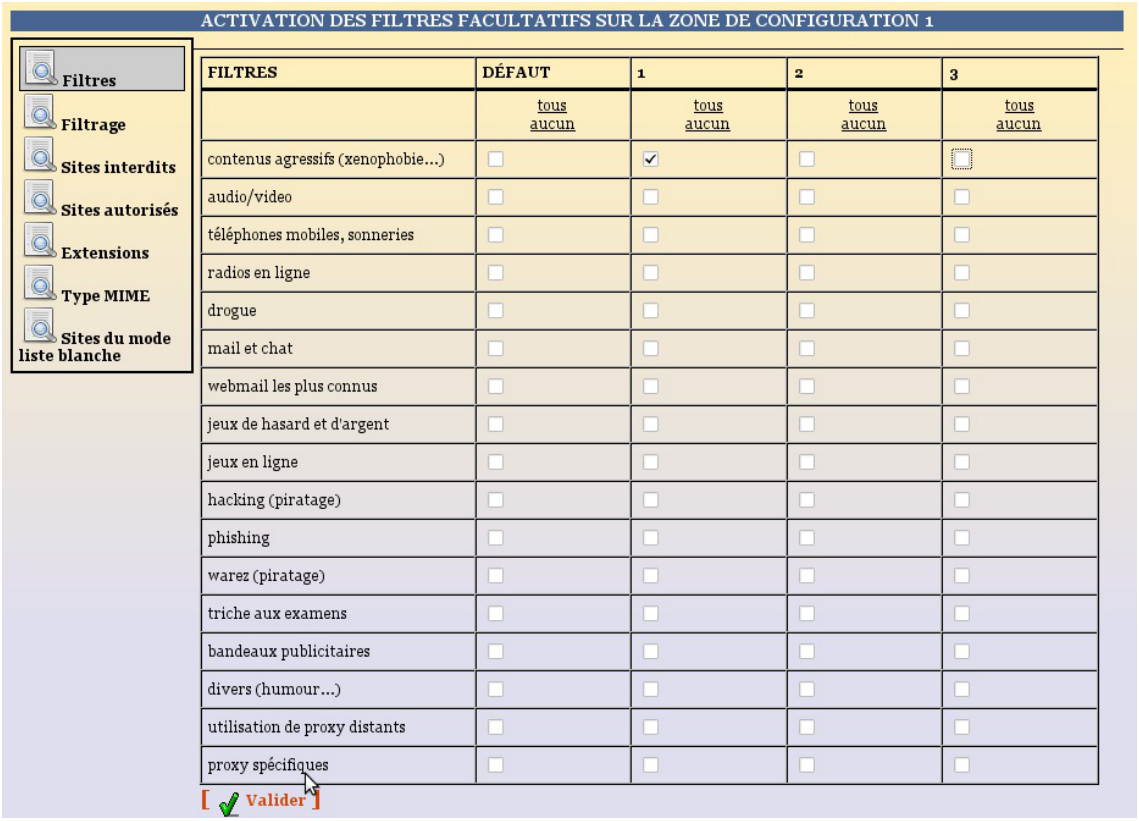
Dans Filtre 1 / Sites / Filtres :

- cocher les quatre cases (pour les quatre politiques de filtrage de la zone 1) ;
- valider.



Activation de filtres optionnels

Pour activer une catégorie seulement pour une politique de filtrage[p.311], seule la case correspondant à la politique doit être cochée.



Restreindre l'activation d'un filtre à une politique

La commande suivante permet de forcer la mise à jour les bases de filtrages :

`/usr/share/eole/Maj-blacklist.sh`

La liste des bases de filtres d'interdiction gérées sur le module EOLE est fournie par le fichier : /usr/share/ead2/backend/config/filtres-opt.

La modification des filtres optionnels activés impactent les fichiers suivants :

- /var/lib/blacklists/dansguardian<num_instance>/f<num_politique>/bannedsitelist
- /var/lib/blacklists/dansguardian<num_instance>/f<num_politique>/bannedurllist

Sur le module AmonEcole, ces fichiers sont dans le conteneur ***reseau*** .

1.4.6. Filtrage syntaxique

Configuration du filtrage syntaxique

Le module Amon filtre dynamiquement les pages web grâce au filtrage syntaxique[p.305].

Ce système de pondération par mot clef se base sur le fichier /var/lib/blacklists/meta/weighted qui est mis à jour toutes les nuits, à partir des données gracieusement gérées et mises à disposition par l'académie de Rouen.

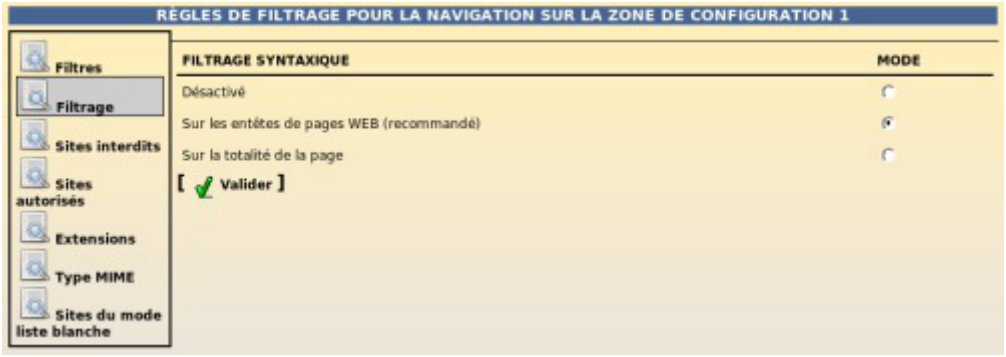
Dans l'EAD, le filtrage syntaxique peut être :

- sur les balises méta[p.302] (par défaut) ;
- sur la page entière ;

- désactivé.

Il est possible de régler ce filtrage pour chaque zone de configuration.

Pour modifier la configuration, aller dans Filtre web 1 / Filtrage.



Configuration du mode de filtrage web pour la zone de configuration 1

Le mode de filtrage syntaxique choisi est enregistré dans le fichier :

/var/lib/eole/config/filtrage-contenu<num_instance>

Mode "safe search" dans les moteurs de recherche

Le proxy utilise un système de réécriture des *URL* afin que le mode "safe search" des principaux moteurs de recherche et sites d'hébergement de vidéos soit activé automatiquement.

http://www.google.com/support/websearch/bin/answer.py?answer=510

Certaines fonctionnalités de recherche avancée ont également été désactivées afin de limiter la charge du serveur.

Filtrage PICS

Le filtrage PICS (http://www.w3.org/PICS) ne s'active automatique que si le filtrage syntaxique est configuré `sur la page entière`.

1.4.7. Interdire et autoriser des domaines

Interdire des domaines et des URL

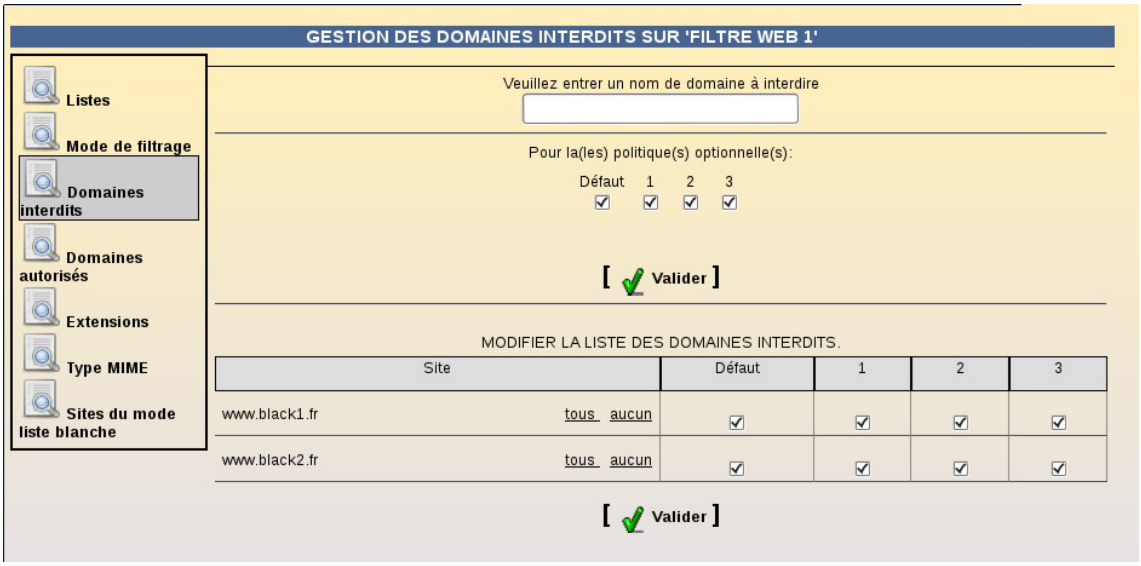
Il est possible de compléter la liste de sites interdits (liste noire[p.307]) en ajoutant des domaines ou des URL sur la liste personnalisée de domaines interdits.

Cette liste est applicable :

- a une zone entière ;
- de manière plus fine sur une seule politique de filtrage.

Le formulaire qui permet d'interdire des domaines est atteignable par le menu portant le nom du filtre choisi dans l'interface de configuration du module, Filtre web 1 par défaut puis Sites / Domaines interdits.

Nommage des filtres dans la configuration du filtrage web : Configuration du filtrage web (cf. Onglet Filtrage web : Configuration du filtrage web) [p.157]



Interdiction de domaines pour les quatre politiques de la zone de configuration sur le filtre nommé par défaut "Filtre web 1"

Les domaines interdits sont écrits dans :

/var/lib/blacklists/dansguardian<num_instance>/f<num_politique>/domains

Sur un module AmonEcole, ces fichiers sont dans le conteneur `reseau`.

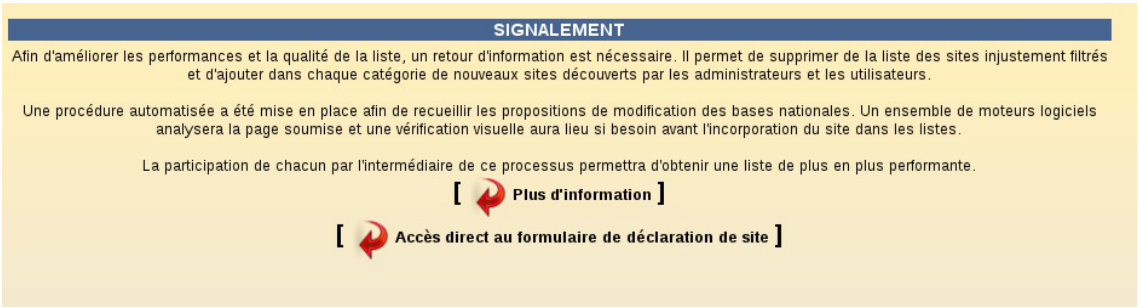
Personnalisations académiques

Des listes de domaines et d'URL peuvent être gérées indépendamment de l'EAD par l'intermédiaire des fichiers suivants :

- /var/lib/blacklists/dansguardian<num_instance>/common/domains_acad
- /var/lib/blacklists/dansguardian<num_instance>/common/urls_acad

Il est possible de signaler des domaines à interdire qui amélioreront les performances et la qualité des bases nationales de domaines interdits.

Pour cela, aller dans `Outils` / `Signalements`.



Vue du formulaire de signalement

Une procédure automatisée a été mise en place afin de recueillir les propositions de domaine à interdire dans les bases nationales.

Un ensemble de moteurs logiciels analysera l'URL soumise et une vérification visuelle aura lieu si besoin avant l'incorporation du domaine dans les listes de domaines interdits.

La participation de chacun à ce processus permet d'améliorer les bases nationales et leur performance et ce afin que chacun puisse en bénéficier.

Il est également possible de faire une signalement directement auprès de l'université de Toulouse 1 Capitole grâce à une formulaire en anglais : http://dsi.ut-capitole.fr/cgi-bin/squidguard_modify.cgi.

Autoriser des domaines et des URL

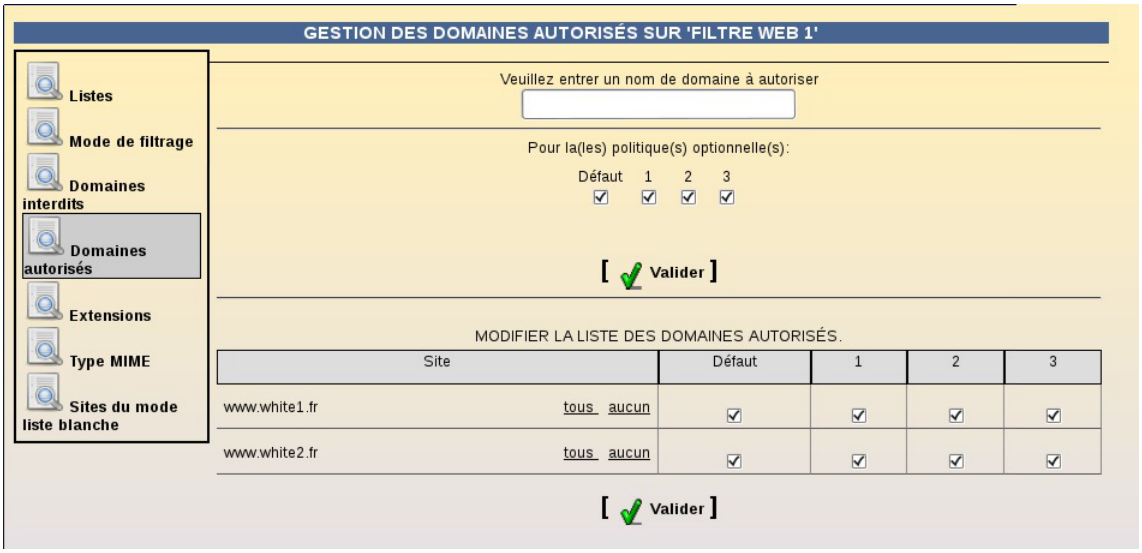
Il est possible de forcer l'autorisation de domaines ou d'URL (liste blanche[p.307]) en les ajoutant à la liste des domaines autorisés.

Cette liste de domaines s'applique :

- sur une zone de filtre web portant le nom du filtre choisi dans l'interface de configuration du module ;
- de manière plus fine par politique de configuration (si des utilisateurs ou des groupes de machine ont été associés à des politiques optionnelles).

Le formulaire se trouve dans `Filtre web 1` / `Sites` / `Sites autorisés`

Le formulaire qui permet d'autoriser des domaines est atteignable par le menu portant le nom du filtre choisi dans l'interface de configuration du module, `Filtre web 1` par défaut puis `Sites` / `Domaines autorisés`.



Autorisation de sites pour les quatre politiques de la zone de configuration sur le filtre nommé par défaut "Filtre web 1"

Les domaines autorisés sont écrits dans :

`/var/lib/blacklists/dansguardian<num_instance>/f<num_politique>/whites`

Sur le module AmonEcole, ces fichiers sont dans le conteneur `reseau`.

1.4.8. Interdire des extensions et des types MIME

Interdire des extensions

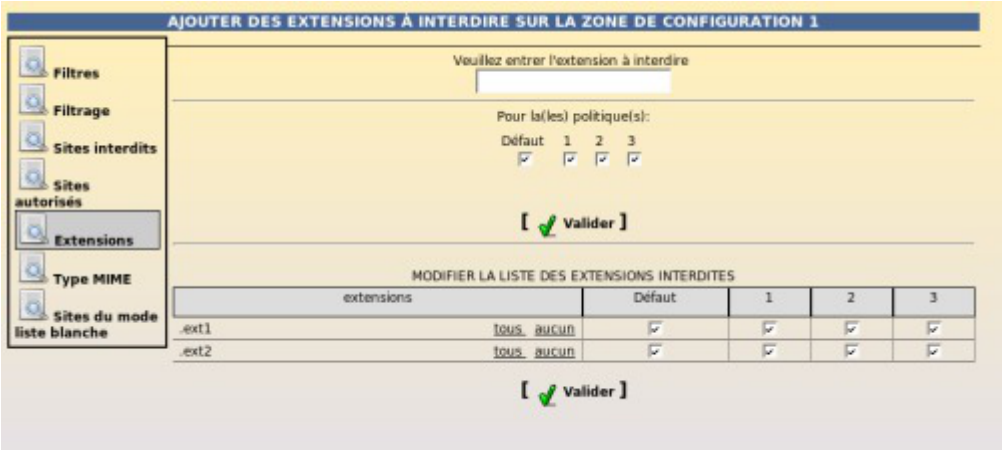
Il est possible d'interdire des extensions, ainsi si l'URL de navigation pointe vers un fichier portant cette extension, l'accès sera interdit.

Cette interdiction s'applique :

- sur une zone de configuration ;

- de manière plus fine par politique de configuration (si des utilisateurs ou des groupes de machine ont été associés à des politiques optionnelles).

Le formulaire se trouve dans Filtre web 1 / Sites / Extensions.



Interdiction d'extensions pour les quatre politiques de la zone de configuration 1

Les extensions interdites sont écrites dans :

/var/lib/blacklists/dansguardian<num_instance>/f<num_politique>/extensions

Sur AmonEcole, ces fichiers sont dans le conteneur ***reseau***.

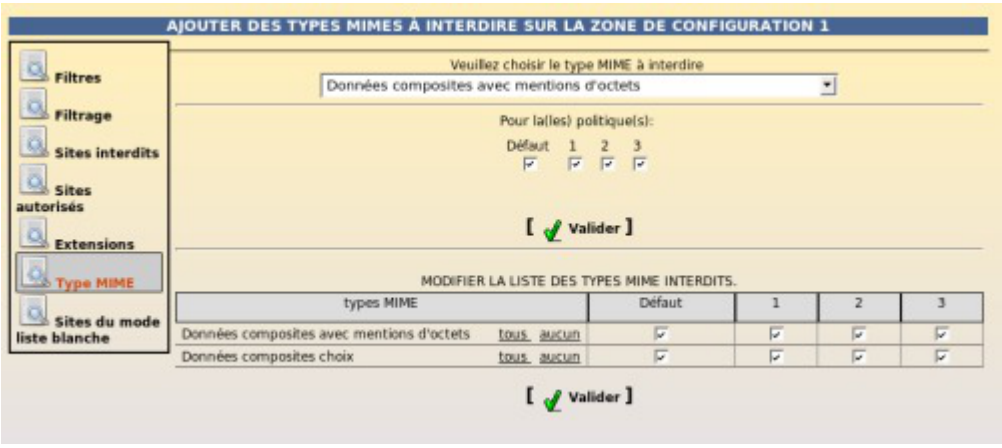
Interdire des types MIME

Il est possible d'interdire des types MIME[p.314]. Cette interdiction fonctionne comme celle des extensions.

Cette interdiction s'applique :

- sur une zone de configuration ;
- de manière plus fine par politique de configuration (si des utilisateurs ou des groupes de machine ont été associés à des politiques optionnelles).

Le formulaire se trouve dans Filtre web 1 / Sites / type MIME.



Interdiction de types MIME pour les quatre politiques de la zone de configuration 1

Les types MIME interdits sont écrits dans :

/var/lib/blacklists/dansguardian<num_instance>/f<num_politique>/types_mime

Sur AmonEcole, ces fichiers sont dans le conteneur ***reseau***.

1.4.9. Politique liste blanche

Le politique liste blanche[p.307] permet de restreindre la navigation web à une liste de sites.

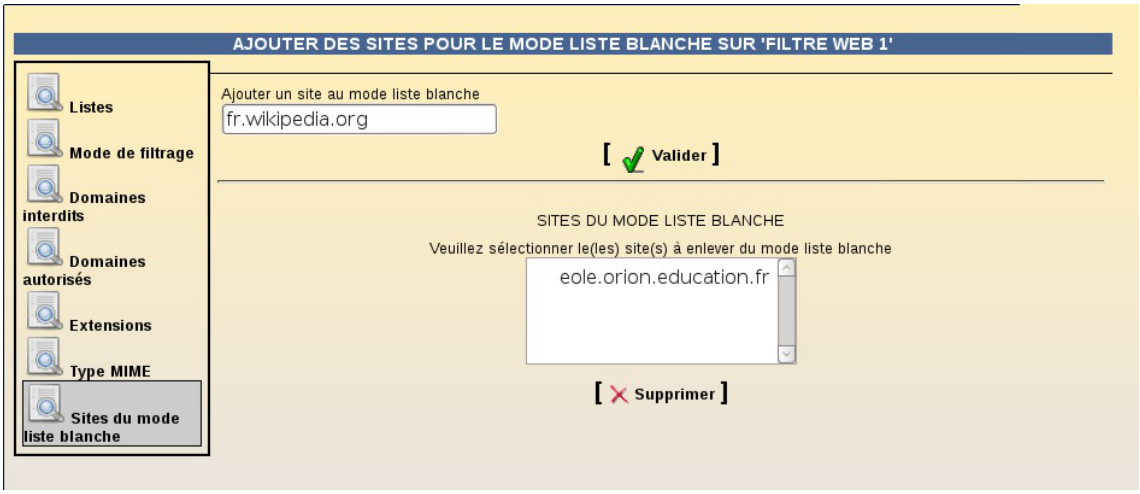
Le principe est "tout est interdit sauf".

Restreindre la navigation au site Wikipédia pour les utilisateurs en mode liste blanche de la zone nommée par défaut "Filtre web 2"

Dans Filtre web 2 / Sites / Sites du mode liste blanche

- ajouter un domaine avec ou sans sous-domaine (exemple fr.wikipedia.org) dans le champ `Ajouter un site au mode liste blanche` ;
- cliquer sur le bouton Valider.

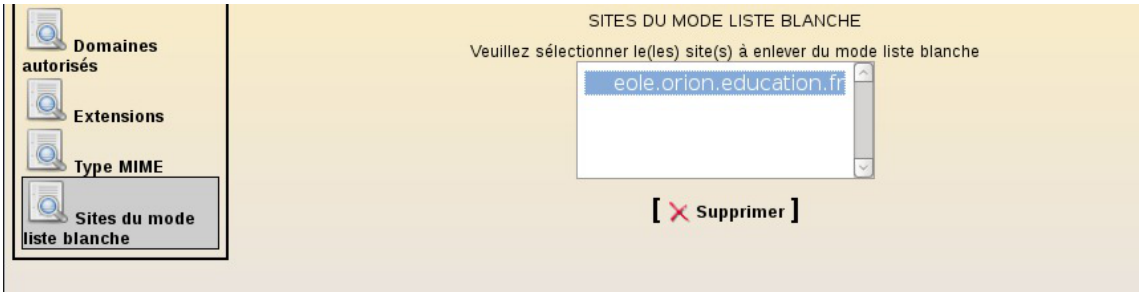
Les utilisateurs et les postes ayant pour politique de filtrage "mode liste blanche" ne pourront naviguer que sur le site ajouté à la liste blanche (exemple Wikipédia).



Ajout d'un site dans la liste blanche

Supprimer un site de la liste blanche

- sélectionner le site dans la liste déroulante `SITES DU MODE LISTE BLANCHE` ;
- cliquer sur la bouton Valider.



Suppression d'un site dans la liste blanche

Les sites de la liste blanche sont écrits dans :

/var/lib/blacklists/dansguardian<num_instance>/f<num_politique>/site_liste_blanche

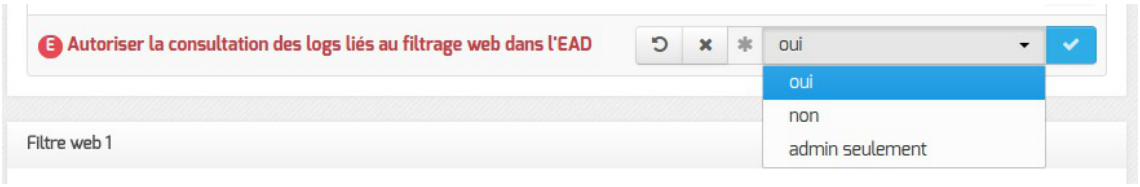
Sur un module AmonEcole, ces fichiers sont dans le conteneur `reseau`.

1.5. Observatoire des navigations

L'observatoire des navigations est un outil de consultation des logs de l'outil de filtrage e2guardian[p.304].

Configuration

L'accès à cet outil se paramètre dans l'interface de configuration du module, dans l'onglet expert : Filtrage web.

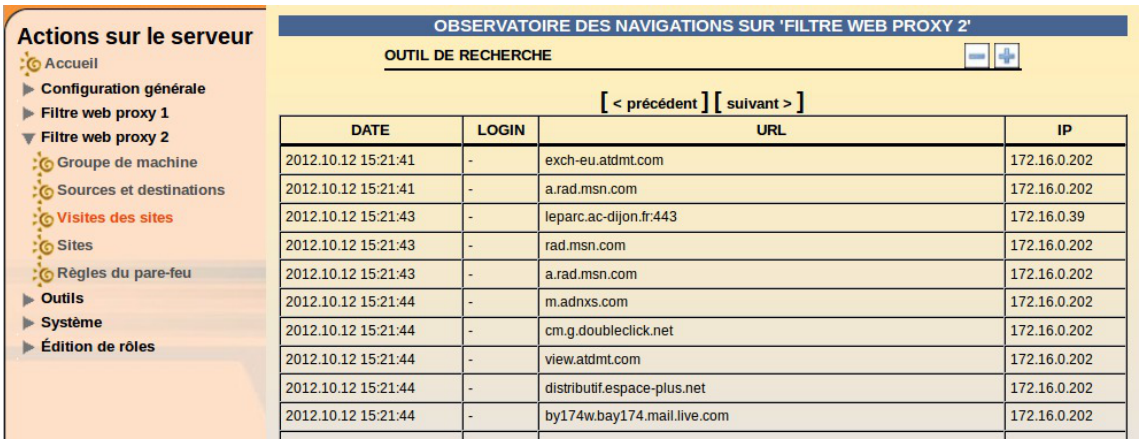


La question `Autoriser la consultation des logs liés au filtrage web dans l'EAD` propose plusieurs options :

- `oui` : accès autorisé pour les utilisateurs EAD possédant les actions `navigation_visit_admin` et/ou `navigation_visit_pedago` ;
- `non` : accès interdit pour tout le monde, personne ne voit le lien Visites des sites (configuration par défaut) ;
- `admin seulement` : accès autorisé uniquement pour le rôle `admin`.

Consultation

La consultation des visites de sites se fait au travers de l'EAD, menu : Filtre web X/visites des sites.



Les noms des menus (ici : Filtre web proxy 2) sont modifiables dans l'interface de configuration du module (variables `dansguardian_ead_filtre1` et `dansguardian_ead_filtre2`).

1.6. Outil d'analyse de logs LightSquid

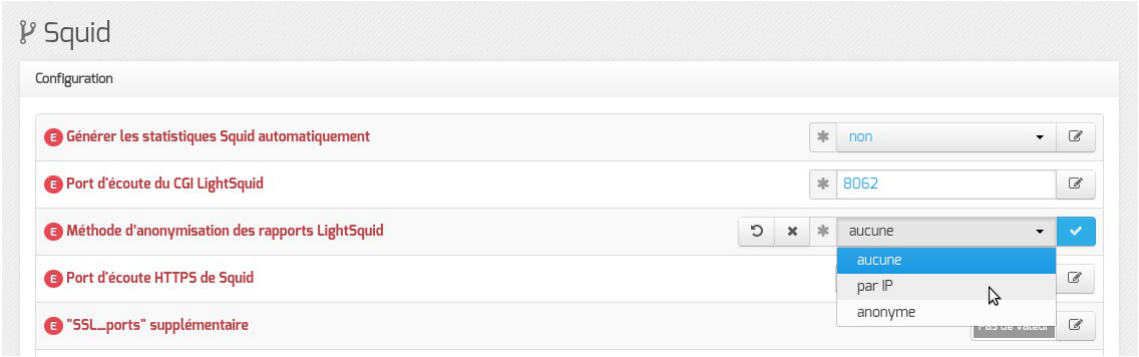
LightSquid est un analyseur de logs pour le proxy/cache Squid[p.313].

Les statistiques générées manuellement ou automatiquement par cet outil sont consultables dans l'interface EAD.

http://lightsquid.sourceforge.net/

Configuration

LightSquid se paramètre dans l'interface de configuration du module, dans l'onglet expert `Squid`. Pour activer la génération automatique des statistiques (toutes les nuits) il faut passer la variable `Générer les statistiques Squid automatiquement` à `oui`. Le port par défaut est 8062.



Paramétrage de Lightsquid

La génération des statistiques proxy peut se faire manuellement, en exécutant la commande `squid_parselogs.sh`.

La méthode d'anonymisation des statistiques générées est également paramétrable :

- `aucune` : aucune anonymisation ;
- `par IP` : n'affiche que les adresses IP ;
- `anonyme` : entièrement anonyme (remplace par un tiret).

Suite à un incident, les statistiques sont celles de la veille, il faut penser à forcer la génération manuellement.

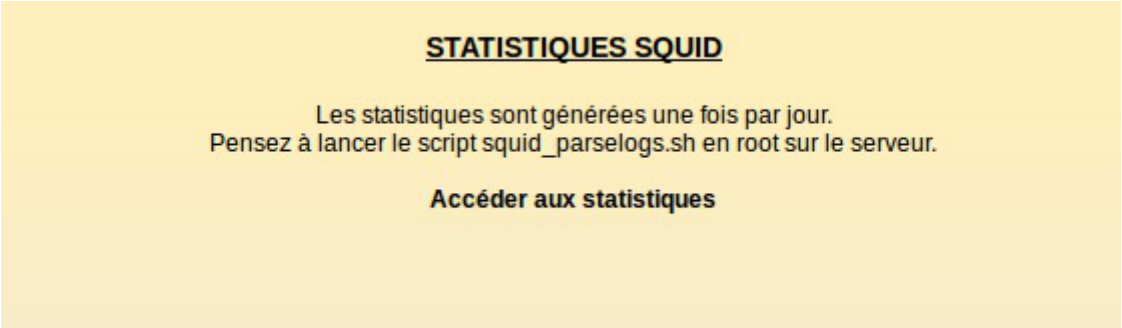
Techniquement, LightSquid fonctionne en mode *cgi* sur un port local (8062 par défaut).

Cela entraîne certaines limitations :

- la ré-authentification nécessaire en mode "pam" ;
- l'accès aux statistiques est impossible depuis un frontend EAD distant.

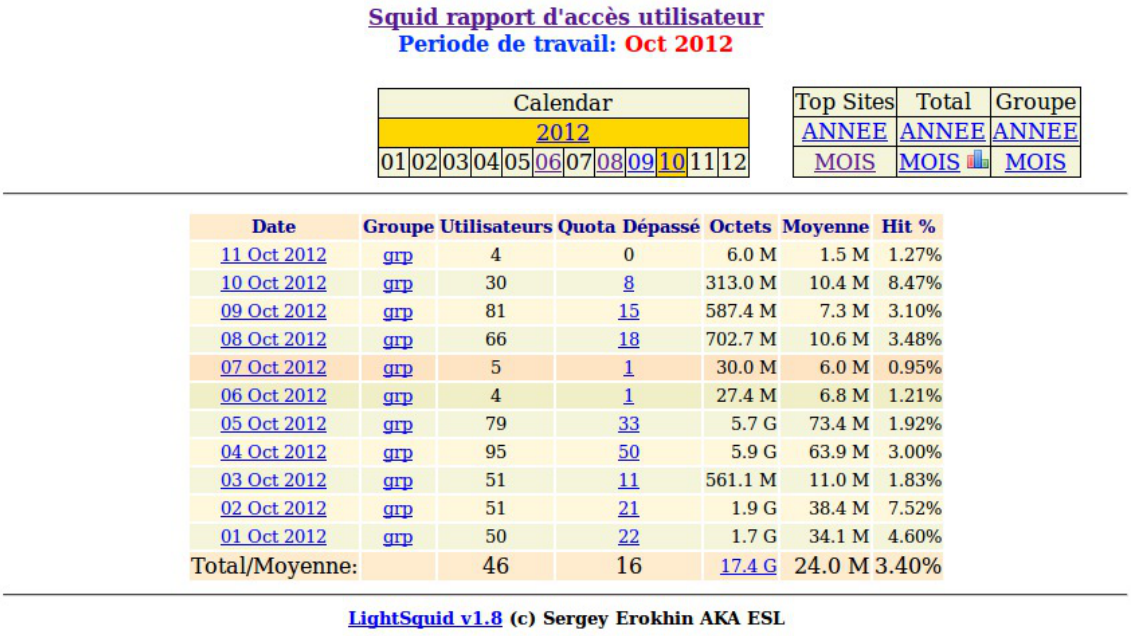
Consultation

La consultation des statistiques LightSquid se fait au travers de l'EAD, dans le menu `Outils` / `Statistiques proxy`.



Pour afficher les statistiques il faut cliquer sur le lien `Accéder aux statistiques`. La navigation se fait dans une nouvelle fenêtre qui demande une authentification. Par défaut, ces statistiques ne sont accessibles que pour le rôle `admin`, un clic sur le bouton `Connexion` sans mot de passe permet de passer à la demande d'authentification pour le compte `root`.

Une fois connecté la vue initiale propose de naviguer dans les statistiques par date (année, jour, mois), par groupe, par quota dépassé.



Consultation au travers de l'EAD

Dans la vue journalière, si la méthode d'anonymisation choisie est par IP, LightSquid n'affiche que les adresses IP utilisées lors de la navigation. Il affiche également le nombre de connexions et le nombre d'octets utilisés. Il est possible d'afficher un rapport sur le top des sites visités et le top des gros fichiers téléchargés dans la journée. Il est possible de repasser à des statistiques journalières par IP.

Squid rapport d'accès utilisateur

Date: **02 Jun 2014 (Rafraîchir :: 04:00 :: 2 Jun 2014)**

Top Sites Rapport

Gros Fichiers Rapport

#	Temps	Utilisateur	Real Name	Connexion(s)	Octets	%	Groupe
1		172.16.0.6	?	1 211	20.8 M	96.3%	?
2		172.16.0.129	?	23	222 384	0.9%	?
3		172.16.0.126	?	12	164 134	0.7%	?
4		172.16.0.134	?	10	130 837	0.5%	?
5		172.16.0.128	?	7	116 574	0.5%	?
6		10.21.58.10	?	80	36 720	0.1%	?
7		172.16.0.135	?	4	19 206	0.0%	?

Vue journalière des statistiques

Dans la vue des statistiques journalières par IP, toutes les adresses visitées par l'utilisateur s'affichent avec le nombre de connexions et les octets consommés.

Squid rapport d'accès utilisateur

Utilisateur: 172.16.0.6 (?)

Groupe: ?

Date: **02 Jun 2014**

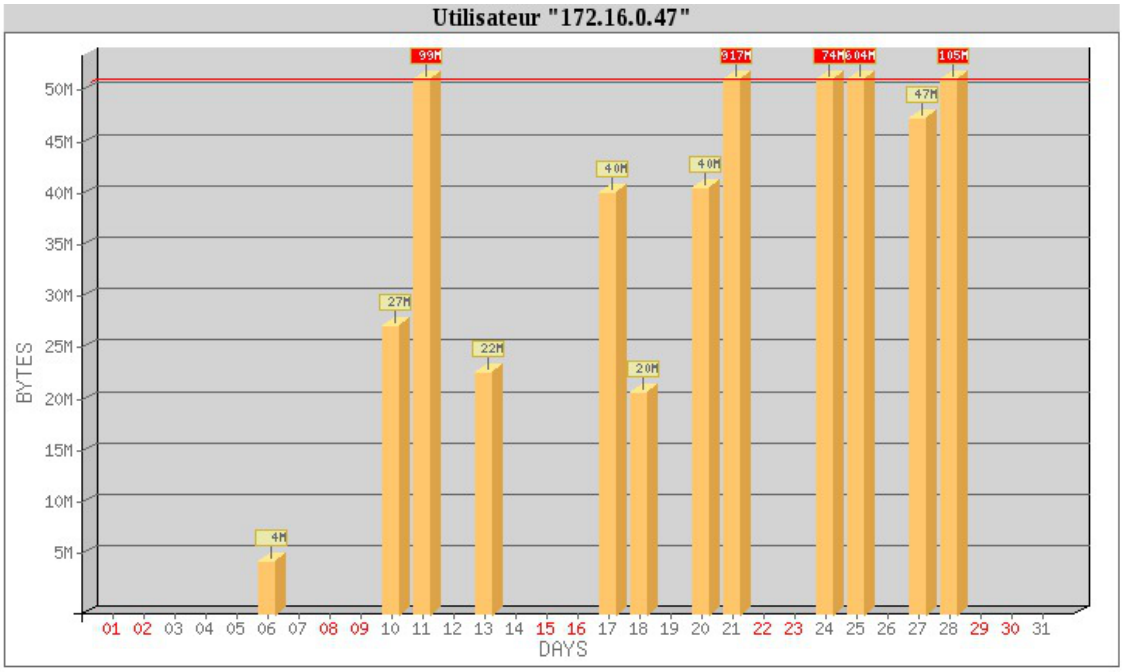
User download "Big Files"

Total **20.8 M**

#	Site(s) Accédé(s)	Connexion(s)	Octets	Somme	%
1	osce106-ilspn25-p.activeupdate.trendmicro.com	28	19.6 M	19.6 M	94.3%
2	osce106-ilspn25wr-p.activeupdate.trendmicro.com	16	869 227	20.5 M	3.9%
3	92.51.156.70	1 152	340 194	20.8 M	1.5%
4	cyberlib.crdp-poitiers.org:443	14	25 142	20.8 M	0.1%
5	ctldl.windowsupdate.com	1	337	20.8 M	0.0%
Total			**20.8 M**		

Vue journalière par IP des statistiques

Dans la vue par mois, un clic sur la consommation total des Octets donne un classement de la consommation d'octets par adresse IP. Dans le tableau affiché, un graphe mensuel de la consommation d'octets par adresse IP est disponible.



Graphe mensuel de la consommation d'octets pour une adresse IP

2. ERA, éditeur de règles pour le module Amon

2.1. Introduction

2.1.1. Présentation

Présentation et fonctionnalités

L'outil EOLE de génération de règles de pare-feu[p.310] pour le module Amon se nomme ERA[p.305].

Il permet de gérer la description de la politique de sécurité d'un pare-feu[p.310]. Cette politique est sauvegardée intégralement dans un fichier de type XML avec un format spécifique à l'application.

Par un processus de compilation, ERA transforme le fichier XML en un bloc de règles iptables[p.306], de manière à instancier ces règles sur un pare-feu[p.310] cible.

ERA et sa documentation sont sous licence libre.

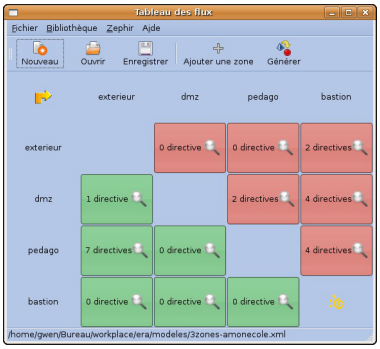
Un logiciel en deux parties

- L'interface de conception permet d'organiser la politique de filtrage et l'enregistre dans un fichier XML ;
- le compilateur génère le script iptables , par compilation, à partir du fichier XML de description du pare-feu.

Seul le format XML est utilisé par le module Amon. L'exportation au format iptables[p.306]

permet d'être utilisable sur un autre pare-feu disposant de Netfilter.

Il n'est bien sûr pas nécessaire de connaître la syntaxe iptables pour manipuler ERA. Le but d'un tel logiciel est justement de s'abstraire de la syntaxe iptables, afin de pouvoir concevoir un pare-feu sans pour autant être un expert. Pour cela, l'interface graphique de ERA est un outil intéressant :



L'interface graphique d'ERA

le fichier lance.firewall

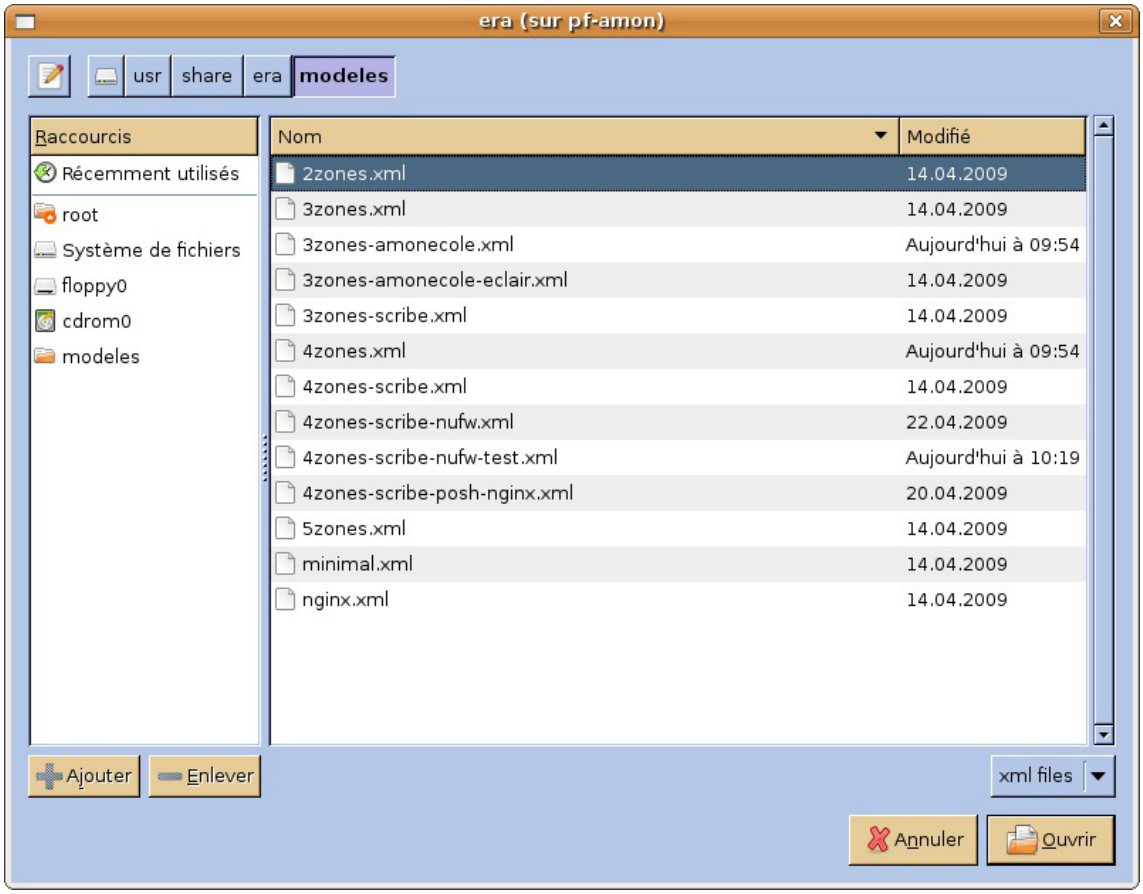
Sur le pare-feu Amon, le fichier `lance.firewall` présent dans `/sbin/` est un fichier de règles iptables qui a été généré par ERA.

Remarquons que si le serveur sur lequel est lancé le compilateur de règles est en mode conteneurs, ERA va générer autant de fichiers de règles iptables que de conteneurs.

2.1.2. Les fichiers XML de modèles

Un modèle[p.308] est un fichier de description du pare-feu. Le format d'enregistrement est un format XML. Divers modèles caractéristiques de description de pare-feu sont disponibles dans le répertoire `/usr/share/era/modeles` et sont des exemples de types de pare-feux (deux, trois, quatre ou cinq cartes réseau).

En général il est préférable, pour commencer un pare-feu, de partir d'un des modèles exemples, et d'y rajouter des directives (ou bien d'en enlever). Partez plutôt du modèle qui correspond au nombre de cartes réseau dont vous disposez sur le serveur.



Boite de dialogue d'ouverture d'un modèle

Lorsque vous modifiez un modèle exemple, il faut impérativement l'enregistrer dans un fichier différent. Sinon, il sera écrasé à la mise à jour suivante.

De plus, il faut que vos nouveaux fichiers XML soient enregistrés dans le répertoire `/usr/share/era/modeles/`.

Charger un modèle à la ligne de commande.

Il est possible d'ouvrir directement un modèle à la ligne de commande. Pour cela, il suffit de spécifier l'option **-f** avec le nom du fichier.

Par exemple :

```
era -f /usr/share/era/modeles/3zones-amonecole.xml
```

Le format XML interne est facilement lisible avec un éditeur de texte (ou un éditeur XML) si l'on est familiarisé avec :

- la notation XML ;
- les différents concepts propres à ERA (tableau des flux, services, directives, ...).

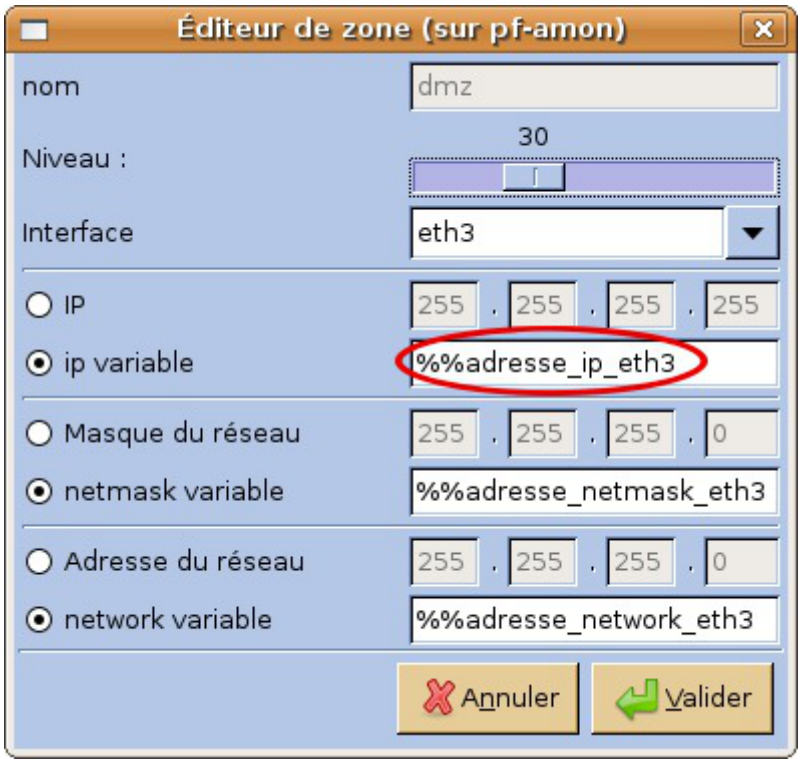
2.1.3. Les variables Creole

ERA[p.305] a été conçu dans le cadre du projet EOLE et pour le pare-feu Amon. Il peut très bien être utilisé en dehors de ce cadre, mais c'est sur un module Amon qu'il devient vraiment possible de déployer toutes les possibilités du logiciel.

Il est possible, à plusieurs endroits de l'interface, d'insérer des variables Creole[p.303] (elles commencent par %%) plutôt que des valeurs fixes.

Le fichier XML de description de pare-feu devient alors un template[p.313] Creole.

Dans la fenêtre d'édition d'une zone, entrer une valeur du type %%ip_variable plutôt qu'une valeur IP fixe.



Une adresse IP de zone peut être templatisée (IP en variable Creole)

Ces variables seront instanciées sur un serveur EOLE. Mais elles peuvent aussi être utilisées pour le déploiement d'autres pare-feux tant que Netfilter est présent.

Limitations de l'intégration entre ERA et Creole

Cette intégration des variables Creole dans ERA a des limites dans le cas des variables multivaluées. Une variable multivaluée au sens de Creole est une variable dont les valeurs sont multiples (c'est une liste d'ips, de networks, etc...).

Il est autorisé d'utiliser des variables multivaluées dans ERA, mais il y a une limitation : si dans une directive donnée plusieurs variables multivaluées sont utilisées (par exemple au niveau d'une extrémité source, d'une extrémité de destination ou d'un service, ou d'un port de redirection...), alors il faut que les autres variables multivaluées utilisées soient déclarées dans le dictionnaire Creole comme esclaves de la première variable multi-valuée, sinon le cas d'utilisation ne sera pas géré.

Le support des groupes de variables multivaluées est très partiel dans ERA, si dans une directive une variable multivaluée est utilisée alors elle doit être déclarée comme maître dans le dictionnaire Creole, et il ne faut pas qu'il y ait dans cette directive une deuxième variable multivaluée **indépendante**, donc les autres variables impliquées sont soit des variables multivaluées esclaves, soit simplement des variables Creole non-multivaluées.

2.2. Utilisation

2.2.1. Les zones de sécurité

Présentation

L'éditeur ERA est un outil de conception par zones[p.315]. Une zone[p.315] correspond physiquement à une carte réseau. Cela permet de découper le parc de machines en réseau ou sous-réseau.

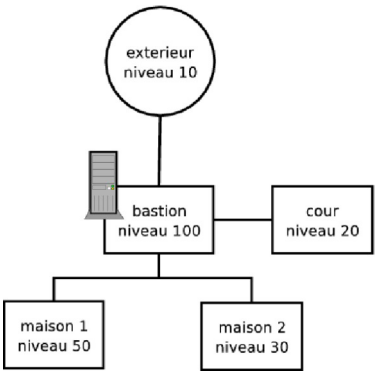
Le pare-feu lui-même étant une zone à part, appelée par convention `bastion`.

Les zones sont ensuite ordonnées par niveau de sécurité[p.309] sous forme d'entiers de 0 à 100.

100 est le niveau de sécurité maximal et correspond à la zone `bastion`. Cela permet de "cartographier" tout le réseau.

Par convention, le niveau de sécurité le plus faible de toutes les zones est affecté à la zone "extérieur".

Les machines de la zone ont un accès complet aux zones de niveau inférieur et aucun accès à celles de niveau supérieur.



Les niveaux de sécurités des différentes zones (vue centrée sur le bastion)

Une zone correspond à un réseau et dans cette zone, on retrouve des sous-réseaux et des machines, correspondant à la notion d'extrémité[p.305] utilisée dans ERA.

Une extrémité est un sous-ensemble d'une zone :

- Elle est définie par un ensemble d'adresses IP ou une adresse réseau.
- Elle hérite du niveau de sécurité de la zone à laquelle elle appartient.

Ajouter une zone

Il est possible à tout moment, même après la conception initiale du modèle, d'ajouter une zone de sécurité. L'ajout d'une zone de sécurité se fait en cliquant sur le bouton `Ajouter Zone` de la barre d'icônes.

Ajouter une zone au tableau des flux

Les cases des noms des zones sont cliquables.

Un clic droit dans une case des noms de zones permet d'afficher les zones ainsi que les extrémités[p.305] qui y sont associées.

Fenêtre d'édition de zone

les trigrammes (préfixes) de zones

Dans le choix des noms de zone :

- les trois premières lettres (trigramme) du nom de la zone sont discriminantes, par exemple : `statistique` et `station` sont des noms de zone incompatibles (c'est la même zone `sta`) ;
- le mot clef `bastion` est réservé (pour la zone du bastion lui-même) ;
- le mot clef `extérieur` est également réservé (pour la zone extérieure, internet).

la gestion des VLAN

Une zone peut aussi représenter un VLAN.

C'est une bonne pratique de créer une nouvelle zone pour gérer un VLAN.

Il n'est pas possible de créer une zone pour tous les VLAN.

S'il y en a plusieurs il faut les créer un à un manuellement.

Syntaxe Creole pour la création des VLAN

Il est fréquent que les valeurs des IP des VLAN soient stockées dans une variable Creole, et que cette variable soit multiple (une variable multiple au sens Creole est une variable qui contient une liste de valeurs). Il faut alors manier correctement la syntaxe Creole pour créer une zone de VLAN.

Exemple de création d'un VLAN de eth1

Dans la widget de création d'une zone, il faut mettre une IP et un netmask variable :

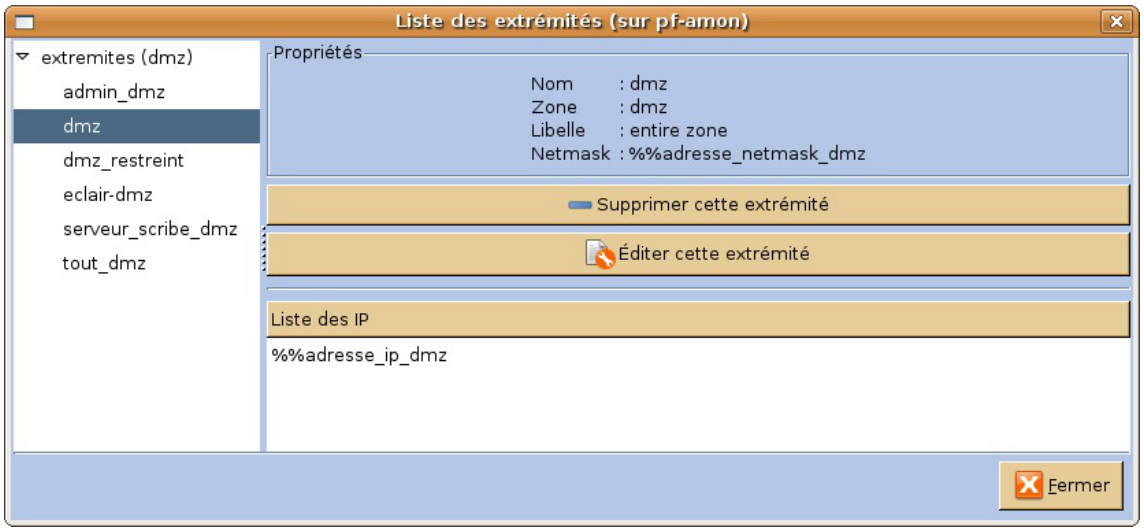
`ip variable : %%id_vlan_eth1[0].adresse_ip_vlan_eth1`

`netmask variable :` `%%id_vlan_eth1[0].adresse_netmask_vlan_eth1`

Ajouter une extrémité

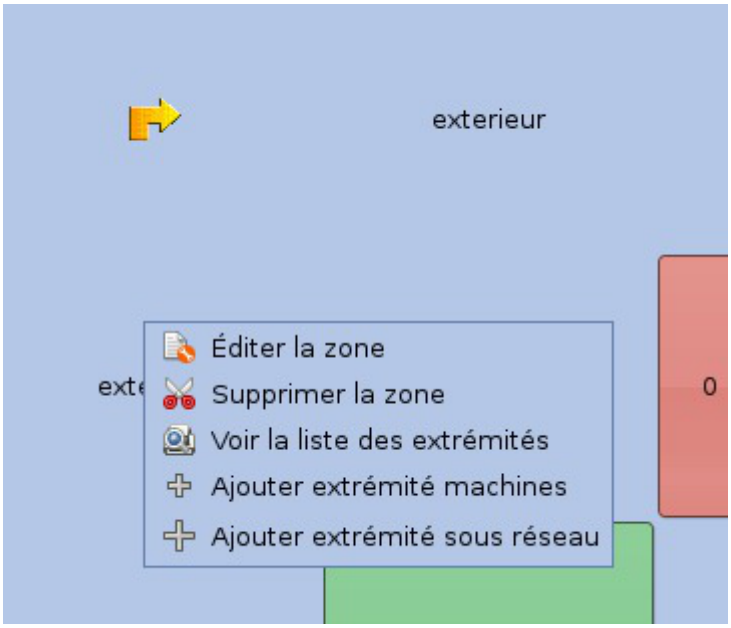
La liste des extrémités est disponible dans le menu bibliothèque / extrémités.

Il est également possible de lister les extrémités d'une zone, en cliquant droit sur le bouton de la zone et en sélectionnant voir la liste des extrémités.

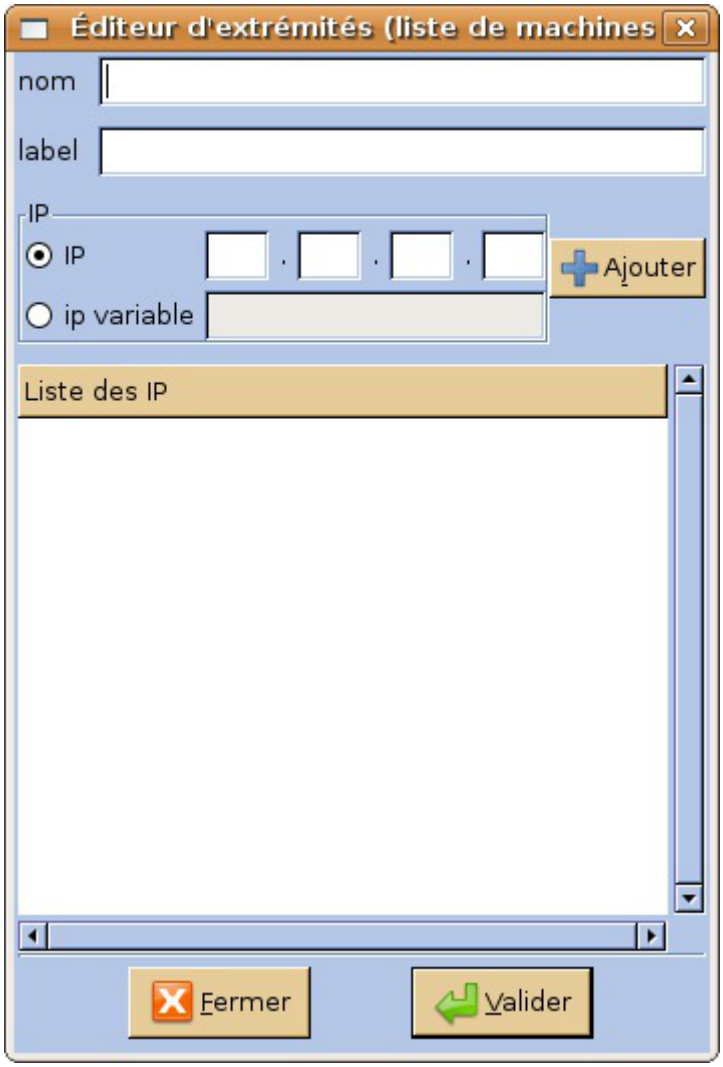


Liste des extrémités

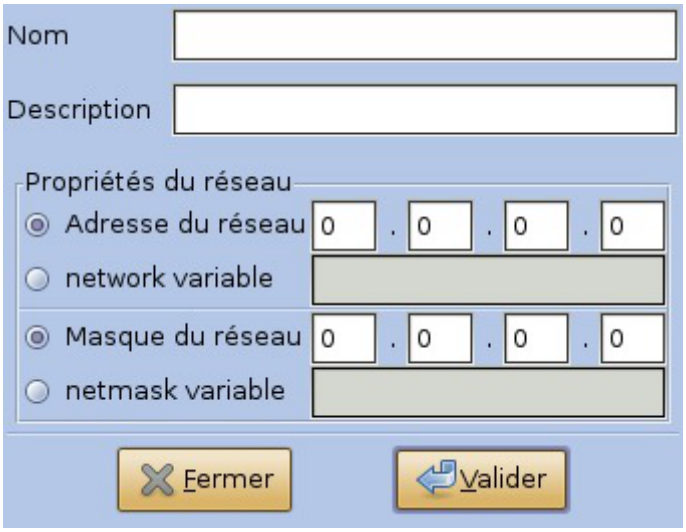
Pour créer une nouvelle extrémité, faire un clic droit dans la zone dans laquelle vous voulez l'inclure. Ensuite, choisir définir un ensemble de machines ou définir un sous-réseau suivant que vous voulez inclure un groupe d'IP ou un sous-réseau.



Un clic droit sur le nom d'une zone affiche le menu contextuel relatif à cette zone



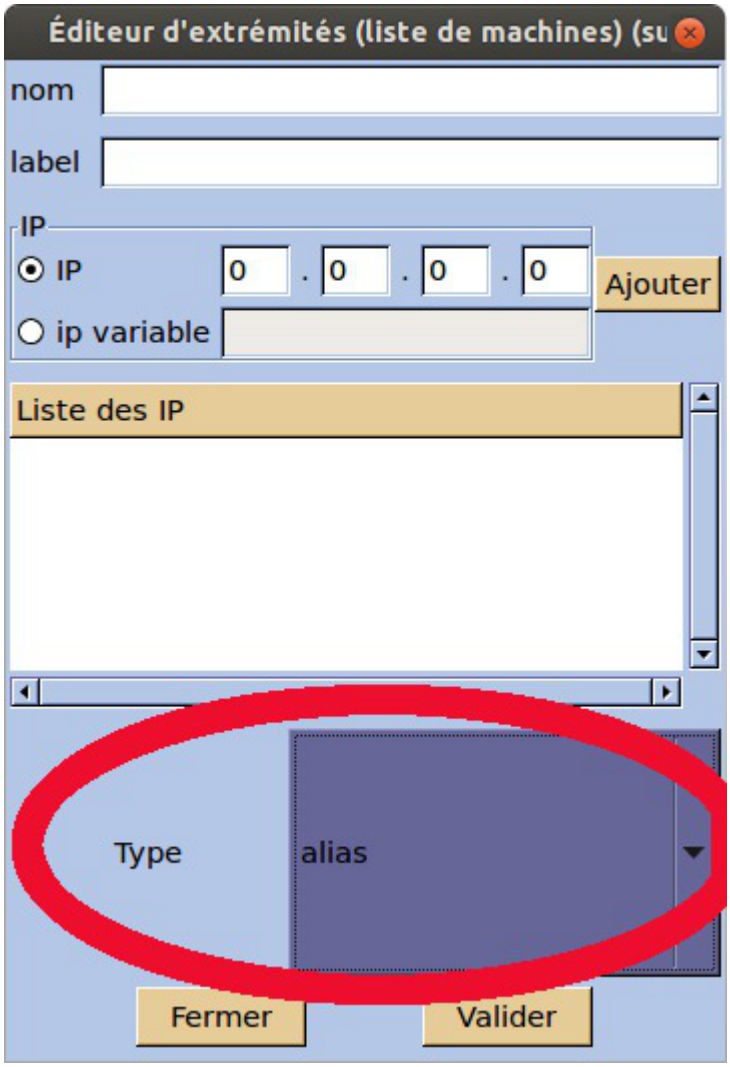
Ajout d'une extrémité dans le cas d'une liste de machines



Ajout d'une extrémité de type sous réseau

Les alias IP doivent être gérés **comme des extrémités** et non comme une zone : **un alias n'est pas une zone**.

Pour ajouter une extrémité de type alias, il faut spécifier le type "alias" dans l'éditeur d'extrémité :



Il est fréquent que les valeurs des IP des alias soient stockées dans une variable Creole, et il est fréquent aussi que cette variable soit multiple (une variable multiple au sens Creole est une variable qui contient une liste de valeurs). Il faut alors manier correctement la syntaxe Creole pour créer une extrémité qui est un alias.

Dans la widget de création d'une extrémité, il faut alors mettre une IP et un netmask variable.

Dans la zone correspondant à la carte, créer une extrémité (clic droit sur la case de la zone).

Un alias de eth2 doit être créé de la façon suivante :

`ip variable : %%alias_ip_eth2[0]`

`network variable : %%alias_network_eth2[0]`

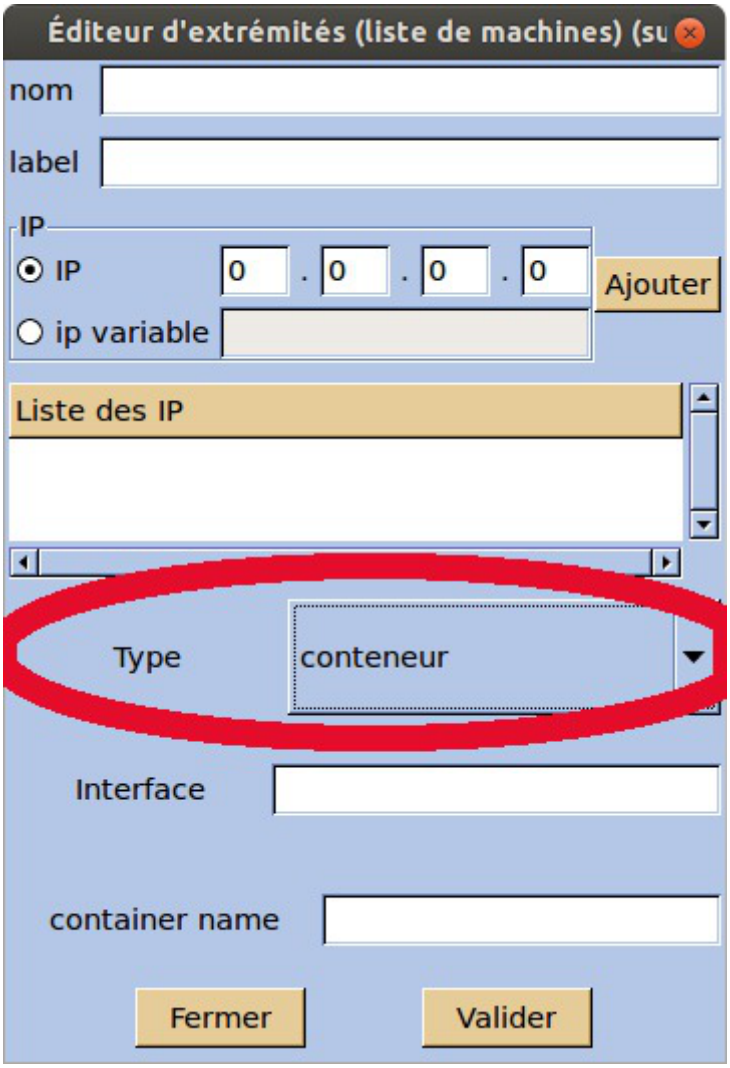
Il sera possible ensuite de créer une directive avec cette extrémité plutôt qu'avec l'extrémité correspondant à l'IP de la zone elle-même.

Les mauvaises fausses bonnes idées pour créer un alias

- créer une zone supplémentaire avec une carte eth0:X ;
- aller de suite dans les inclusions statiques ;
- utiliser la variable eth0 de Creole comme IP multivaluée.

Les extrémités de type conteneur

Il est possible également de créer une extrémité dans la zone **bastion**. Dans la zone bastion il y a depuis la version 2.4 un nouveau type d'extrémité, le type **conteneur**. Ce type d'extrémité permet de créer des directives à destination des conteneurs (directives de type INPUT).



Une extrémité de type conteneur est à destination du conteneur. Elle nécessite deux informations : le nom de l'interface (typiquement : "br0", "eth1", ...), et le nom du conteneur (typiquement : "bdd", "internet"...)

2.2.2. Les flux

Présentation

Dans ERA, les règles sont systématiquement classées d'après la zone d'origine et la zone de destination. ERA est donc conçu autour du concept de flux[p.306] plutôt que centré sur la notion de règle. Par voie de conséquence, chaque zone est reliée à une autre zone par des flux.

A l'intérieur d'un flux, on trouve deux flux orientés, le "flux montant[p.306]" et le "flux descendant[p.306]".

Les "flux montants[p.306]" concernent les zones[p.315] d'un niveau de sécurité plus faible vers un niveau de sécurité plus élevé, et réciproquement pour les "flux descendants[p.306]".

Pour pouvoir ordonner les flux en vue d'une cohérence globale, il convient ensuite de modéliser le "

tableau des flux[p.313]".

Ce tableau correspond à l'ensemble des flux du modèle de sécurité à l'intérieur duquel seront rangées les règles (ou directives).

	10	20	100
10		Montant	Montant
20	Descendant		Montant
100	Descendant	Descendant	

Directives montantes et descendantes dans la matrice de flux

Lorsque les flux montants et les flux descendants sont définis, une politique par défaut est automatiquement spécifiée. Ici, la politique de sécurité par défaut qui résulte de la matrice de flux est :

	10	20	100
10		Interdit	Interdit
20	Autorisé		Interdit
100	Autorisé	Autorisé	

Repérage des types de directives (autorisation ou interdiction) dans la matrice de flux

Niveaux de sécurité égaux

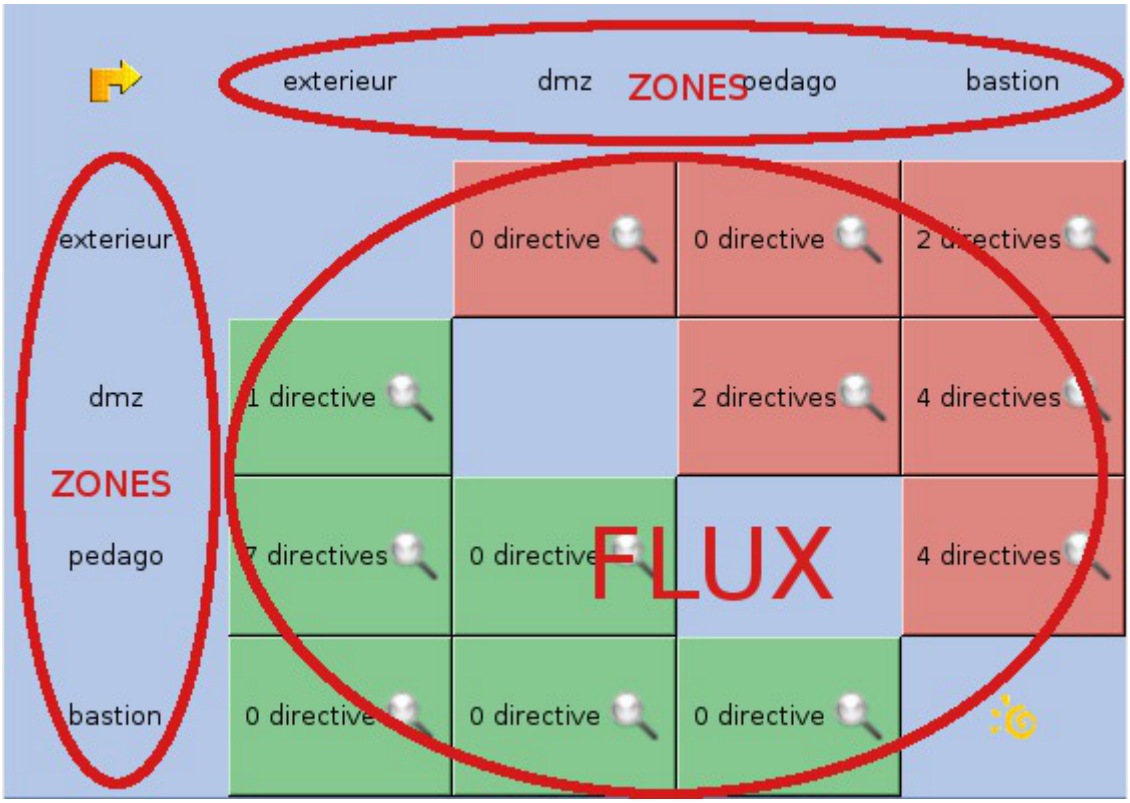
Lorsque deux zones ont deux niveaux de sécurité égaux, alors la politique par défaut est une interdiction des deux côtés (flux montants et descendants).

Changement de la politique par défaut

Il est possible d'inverser le comportement de la politique par défaut. On peut choisir d'interdire les flux d'une zone vers une autre par défaut.

L'interface de conception

La fenêtre principale représente un tableau composé de cases de zones et de cases de flux.



Interface d'ERA avec un modèle chargé

Les cases des flux sont colorés. Les cases de couleur verte sont en "autorisation" par défaut et les cases de couleur rouge sont en "interdiction" par défaut.

La couleur rouge indique que le flux orienté est interdit, tandis que la couleur verte montre que le flux orienté est autorisé.

2.2.3. Les directives

2.2.3.a. Présentation

Une directive[p.308] est une règle concernant un service ou un groupe de services entre deux extrémités.

Cette règle peut être de type "interdiction", "redirection", "source NET" ou "destination NAT".

2.2.3.b. Les services et les groupes de services

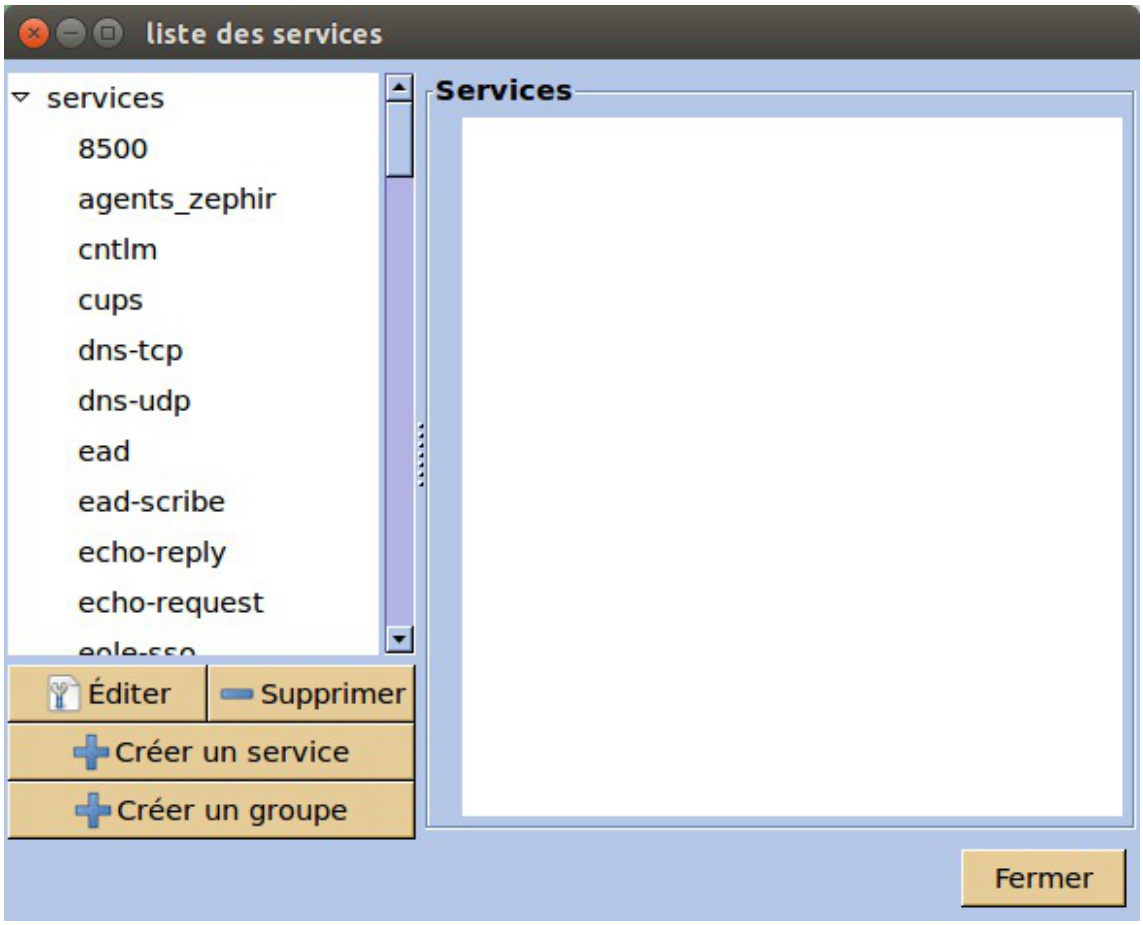
Avant de pouvoir créer une directive, il faut d'abord créer un service[p.313].

Par exemple, le service "serveur web" est défini par le protocole HTTP sur le port 80.

Il y a déjà une bibliothèque de services prédéfinis dans ERA.

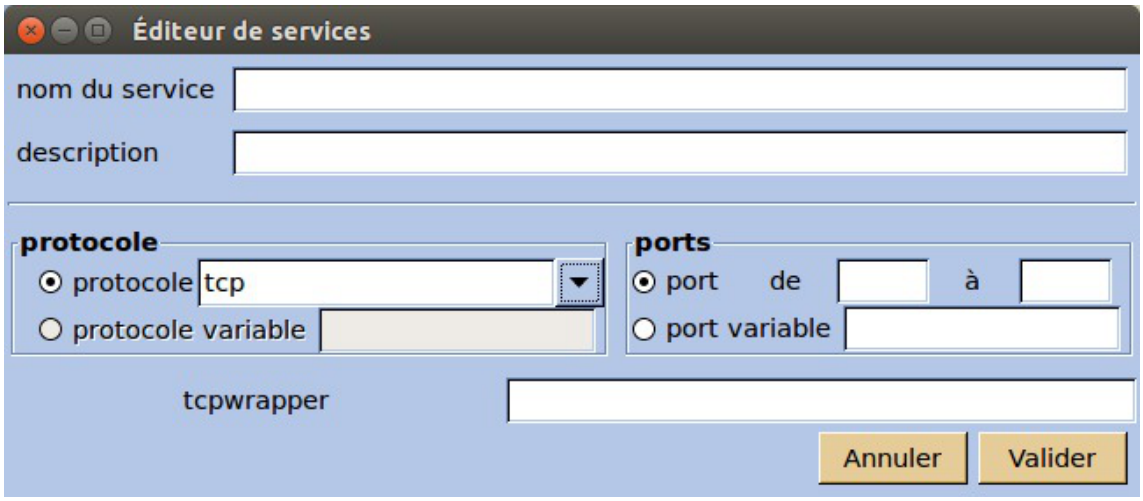
Pour lister ces services, aller dans le menu : Bibliothèque > services.

Pour créer un service, aller dans le menu : `Bibliothèque > services`.



Liste et édition des services

Créer ou modifier un service signifie renseigner les noms, descriptions, protocoles et ports.



Ajout d'un service

Remarquons que si on choisit un port égal à 0, cela équivaut à saisir de 0 à 65535.

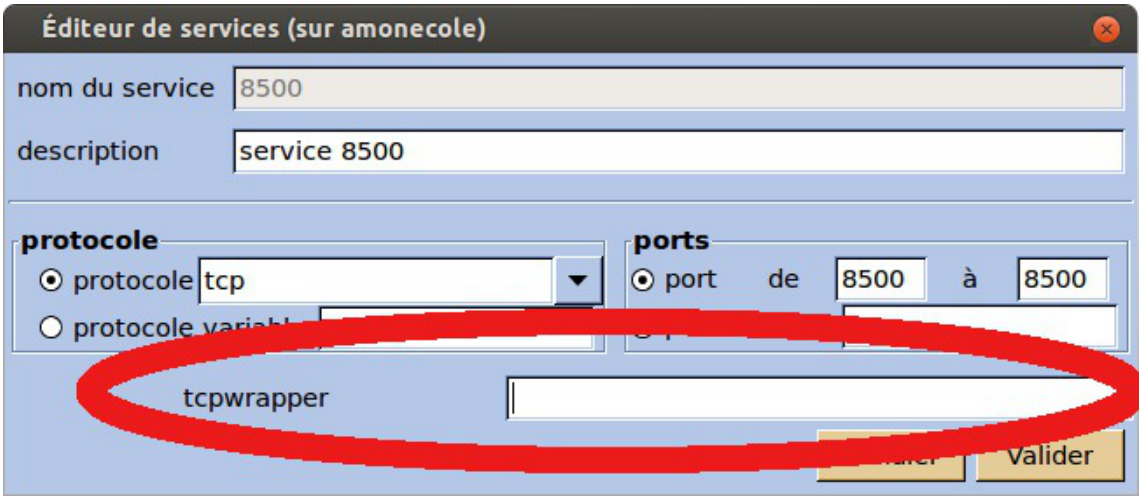
Si on veut que le service ne concerne qu'un seul port, il faut mettre deux fois le même numéro de port.

Depuis EOLE 2.4, l'utilisation d'une variable Creole pour définir le type de protocole à utiliser n'est plus fonctionnelle.

Cette fonctionnalité n'est plus disponible dans l'interface à partir d'EOLE 2.6.

implémenter un service avec tcpwrapper

Pour prendre en compte le tcpwrapper avec ERA, ça se passe au niveau des services. Il suffit de renseigner le nom tcpwrapper du service (le nom tel qu'il doit apparaître dans le fichier **hosts.allow**) et le tcpwrapper sera pris en compte dès qu'une directive utilisant ce service sera créée.

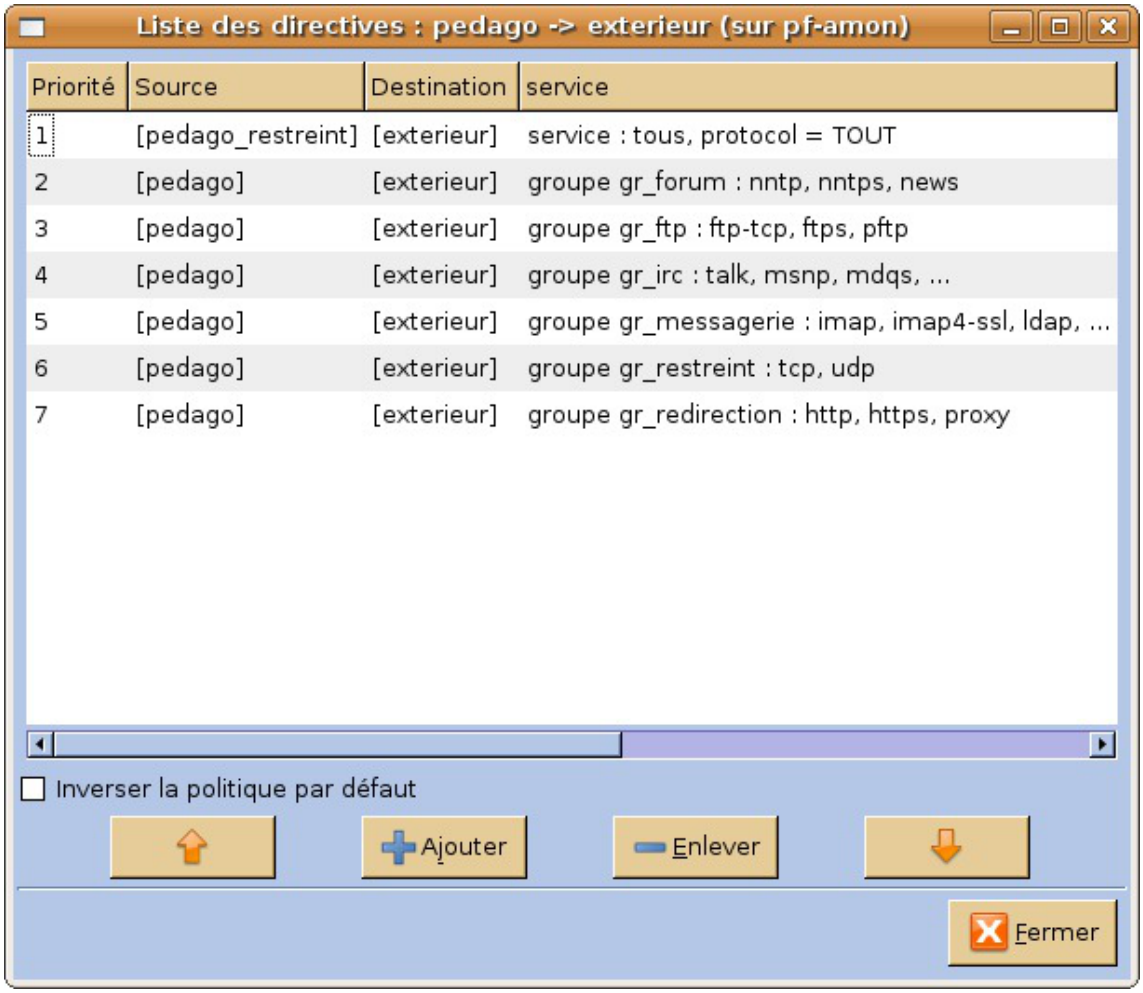


le tcpwrapper en mode conteneur

Remarquons que ERA va générer un fichier tcpwrapper, classiquement le fichier /**etc**/**hosts.allow**, mais que en mode conteneur autant de fichiers seront générés que de conteneurs.

2.2.3.c. L'éditeur de directives

Un clic droit ou un double clic dans une case de flux du tableau permet de visualiser la liste des directives de façon synthétique.

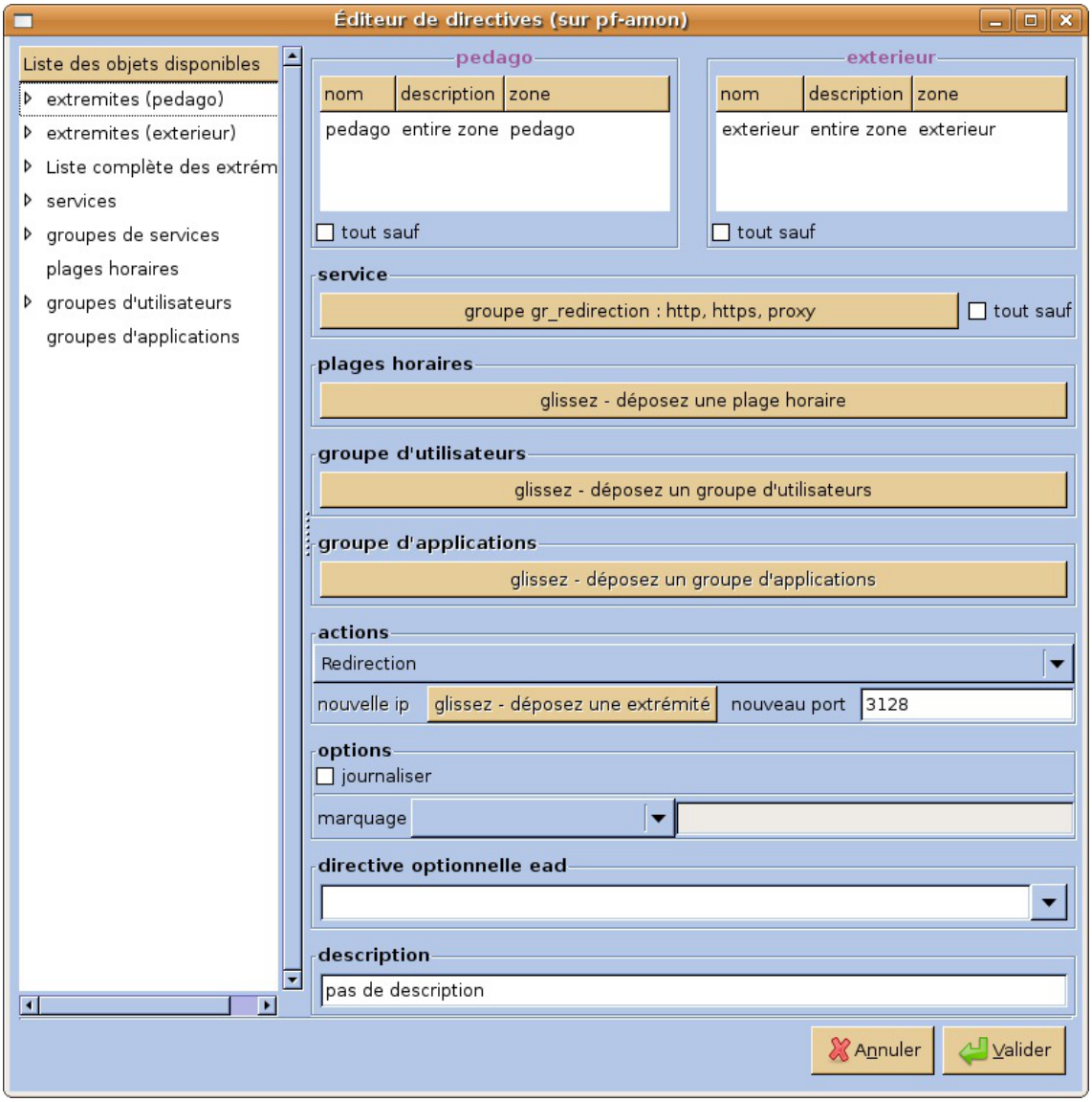


Fenêtre de liste des directives dans un flux donné

Les directives sont triées par ordre croissant. C'est l'ordre dans lequel seront appliquées les règles sur le pare-feu cible.

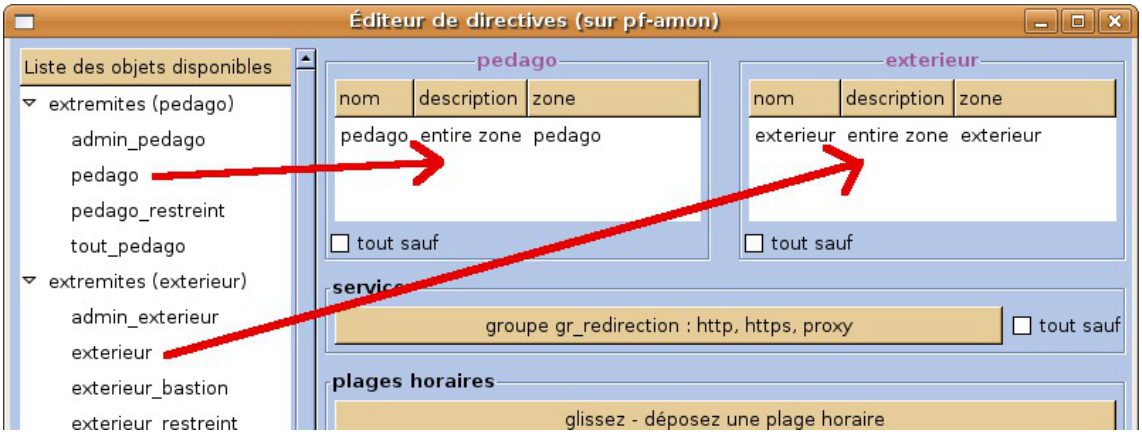
Les directives de `nat` et `redirection` sont appliquées forcément avant les autres. Ceci est le comportement de Netfilter[p.308].

Depuis cette fenêtre, il est possible d'éditer une nouvelle directive (en double-cliquant dessus) ou d'en ajouter une si nécessaire.



Fenêtre d'édition des directives

Pour construire une directive, il faudra au moins deux extrémités (entre deux zones) et un service (ou groupe de services), qui doit être renseigné par glisser-déplacer.



Glisser-déposer d'une extrémité pour la source et la destination d'une directive

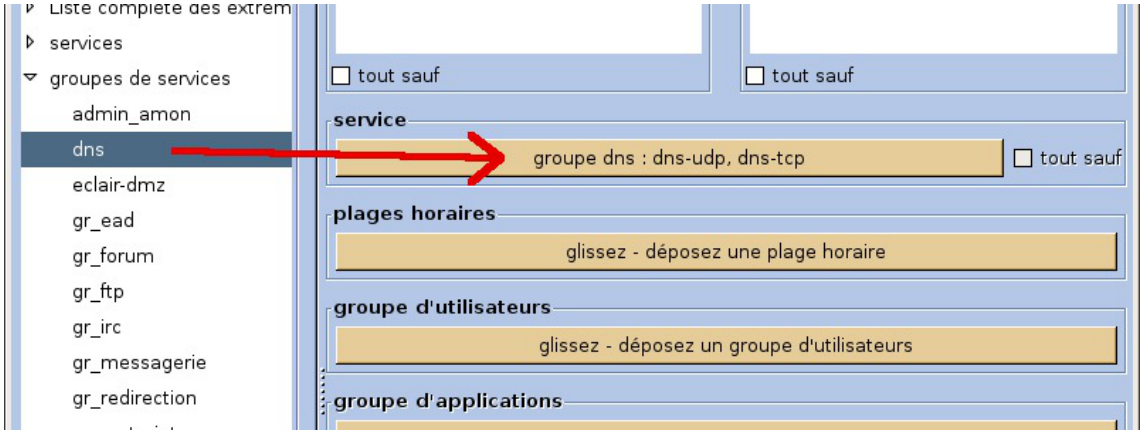
Si vous ne renseignez pas les extrémités, c'est la zone entière qui est prise (plus précisément l'extrémité désignant la zone entière).

Différence entre zone entière et zone restreinte

La zone entière est le réseau correspondant à une carte réseau du pare-feu. Cela correspond au réseau local ainsi que d'éventuels sous-réseaux derrière une passerelle. Elle est nommée *<nom de la zone>*.

La zone restreinte ne correspond qu'au sous-réseau. Elle est nommée *<nom de la zone>_restreint.*

A chaque directive est associé un service ou un groupe de services qu'il est nécessaire de renseigner par glisser-déposer.



Sélection d'un service depuis l'éditeur de directive

> Les types de directives

Les types de directives

Il y a plusieurs types de directives :

- autorisation
- interdiction
- redirection
- SNAT
- DNAT
- FORWARD

Les directives d'autorisation et d'interdiction

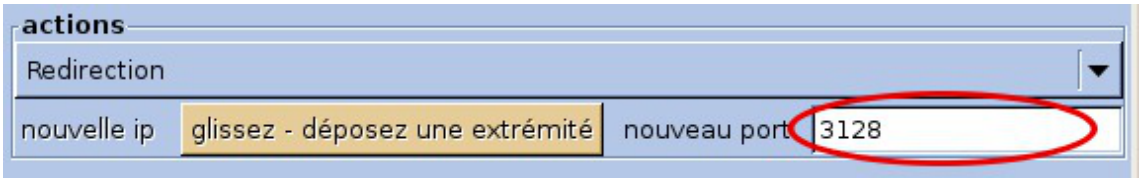
Une directive est dans une case de flux et elle s'oppose à la politique par défaut du flux. Si le flux est en autorisation, la directive propose une interdiction et inversement.

Type standard de directive (autorisation/interdiction)

En plus du filtrage simple, d'autres fonctionnalités sont proposées.

Les directives de redirection

Une directive de type redirection permet de rediriger une requête d'un port déterminé vers un port de la machine elle-même (bastion).



Directive de redirection

Cette fonctionnalité est particulièrement intéressante dans le cas du proxy transparent. Toutes les requêtes destinées à des serveurs web seront redirigées automatiquement vers le service proxy installé sur le serveur.

Les directives de DNAT/SNAT

Le NAT permet de modifier l'adresse source (SNAT) ou destination (DNAT) d'une requête.

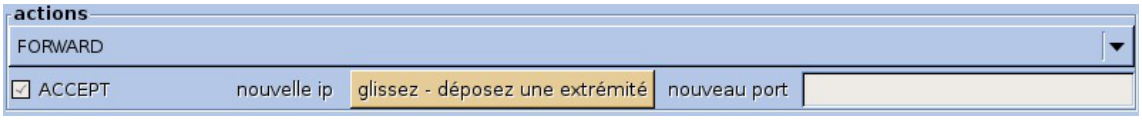
Glisser-déposer de l'extrémité de redirection

Le SNAT est utilisé pour toutes les requêtes provenant de la zone pédago vers l'extérieur. Cela permet de transformer les adresses source locales en adresses source extérieures.

Le DNAT et le SNAT ne sont pas autorisés si la directive est authentifiée.

Les directives FORWARD

Le FORWARD permet d'autoriser la translation un réseau vers un autre



> Les plages horaires

Création d'une plage horaire

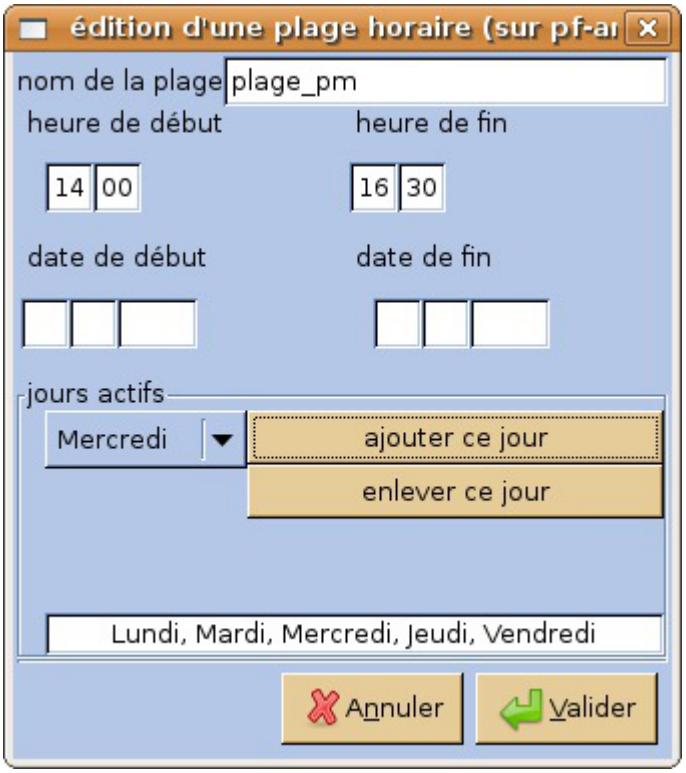
Les plages horaires sont définies depuis le menu `Bibliothèque > plage horaire`.

Il y a trois manières de définir une plage horaire :

- les heures de début et de fin ;
- les dates de l'année de début et de fin ;

- les jours de la semaine.

Les informations indispensables sont : le nom et une ou plusieurs de ces trois manières.



Ajouter des plages horaires

Affectation d'une plage horaire à une directive

Il est possible de définir une plage horaire à l'intérieur de laquelle la directive sera activée.

Depuis l'éditeur de directives, glisser-déposer une plage horaire. Affecter une plage horaire à une directive.

La plage horaire d'une directive

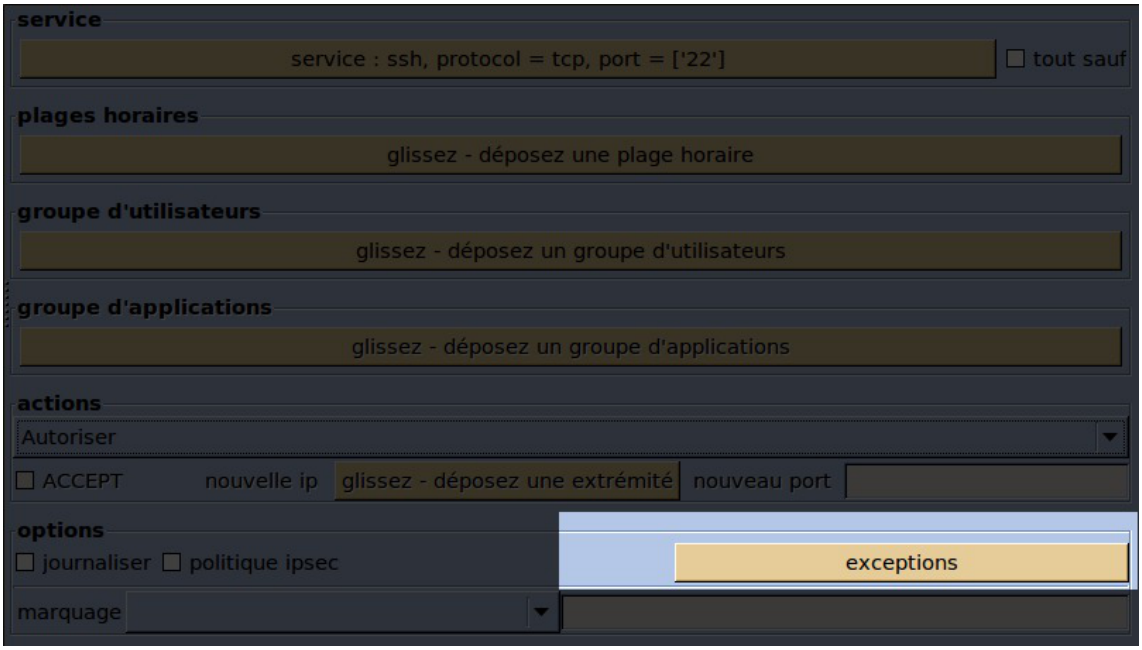
> La journalisation

La case "journaliser" permet de tenir un journal des évènements (logs) de la directive (grâce à ULOG).

Journaliser la directive

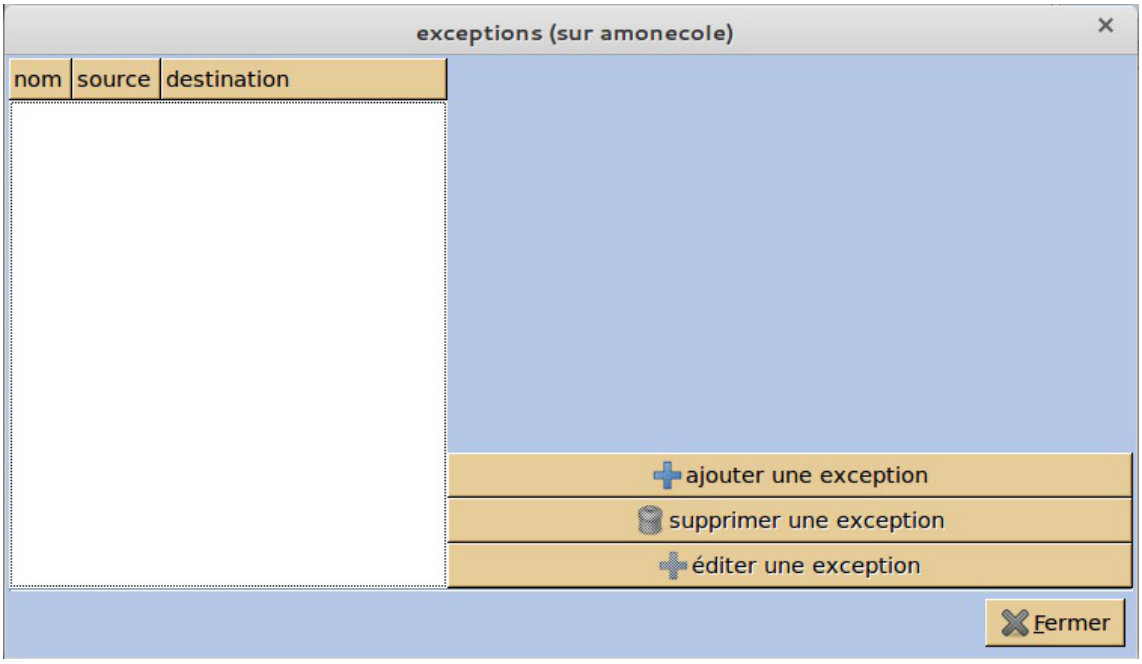
> Gérer des exceptions

Dans l'éditeur de directives il est possible d'ajouter des exceptions.



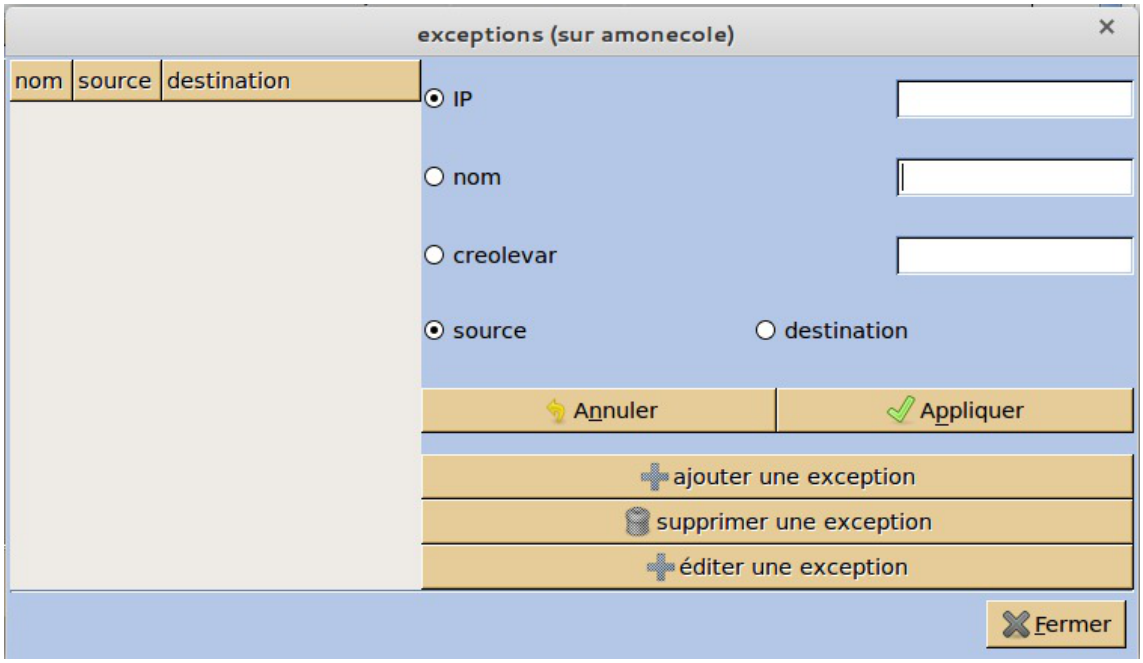
L'éditeur d'exceptions permet :

- d'ajouter une exception ;
- d'éditer une exception ;
- de supprimer une exception.



L'exception peut se faire :

- sur une adresse IP ;
- sur un nom de domain ;
- sur une variable Creole.



> Le marquage

Le marquage est une fonctionnalité avancée de iptables[p.306] permettant d'identifier un paquet grâce à une marque spécifiée dans l'interface.

> Les directives optionnelles

Présentation

Une directive optionnelle[p.304] est une directive qui va être activable ou désactivable depuis l'interface EAD[p.304].

Pour cela, il est indispensable d'affecter un libellé optionnel à cette directive. Il est aussi possible de choisir un libellé optionnel préexistant dans la liste des libellés affectés aux directives, ce qui crée une notion de groupe de directives optionnelles.

La directive est étiquetée comme optionnelle

Un libellé optionnel sert de tag (d'identifiant). Il peut être composé de caractères alphanumériques [1-9] [a-z] [A-Z] et éventuellement de "_" ou d'espaces. Il est impératif de ne utiliser d'autres caractères accentués.

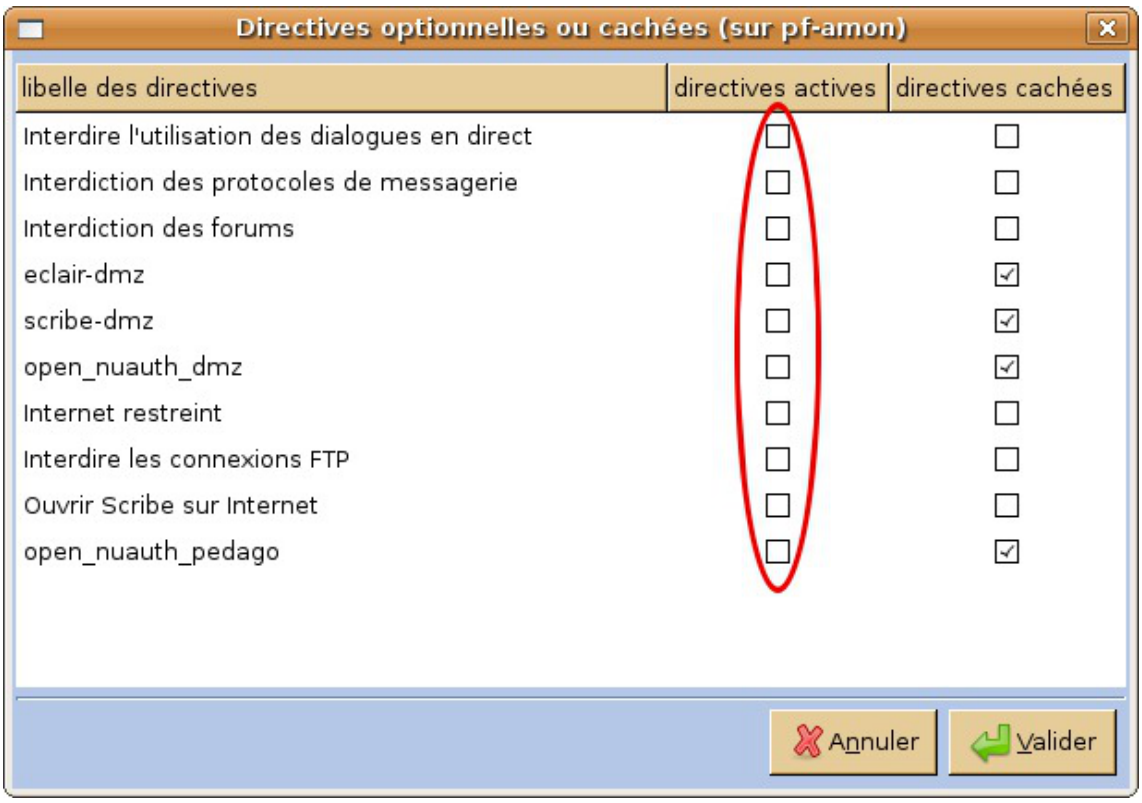
Directive optionnelle active

Une directive optionnelle n'est pas active par défaut dans ERA, c'est-à-dire que la directive ne sera pas appliquée sur le serveur cible. Pour l'appliquer, il faut aller la cocher comme active dans l'interface EAD.

Mais il est possible de rendre une directive active par défaut dans ERA. Dans ce cas, il faudra aller dans l'interface EAD pour la désactiver.

L'état actif et la possibilité de marquer une directive comme optionnelle sont deux notions différentes.

Pour activer une directive, aller dans `Bibliothèque` / `Directives optionnelles`.



Fenêtre de la bibliothèque permettant d'étiqueter une directive comme optionnelle

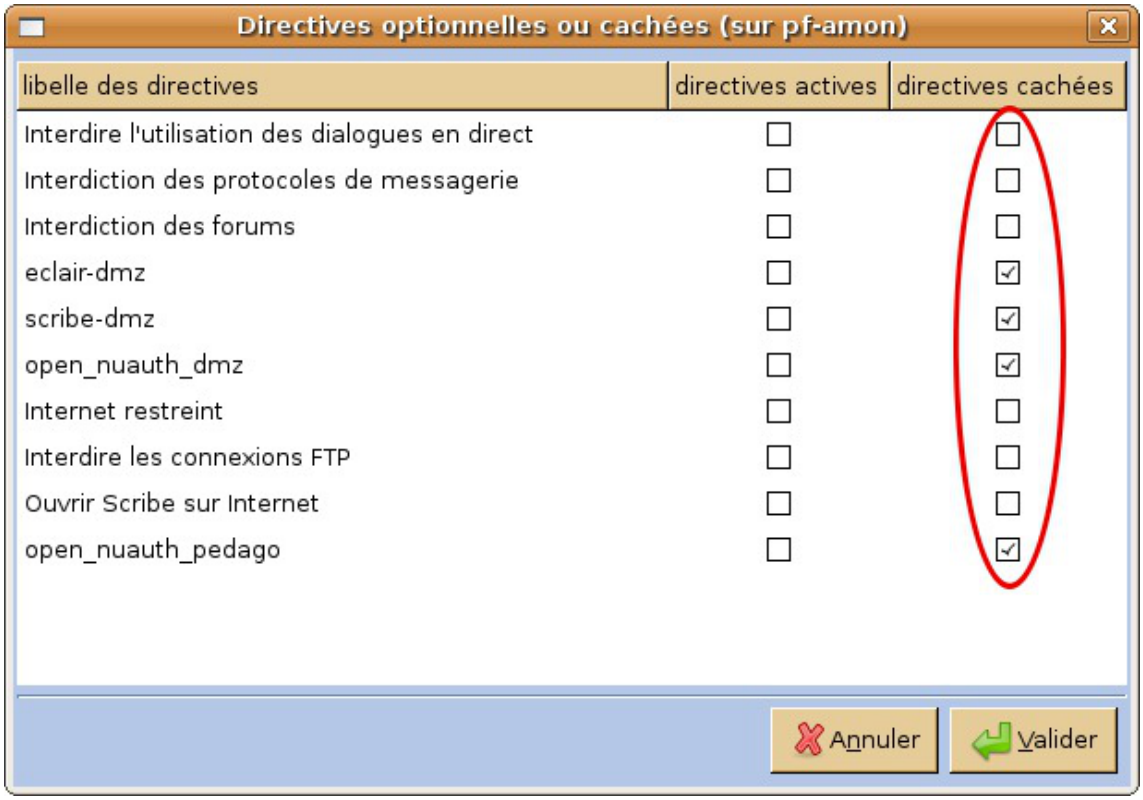
Directive optionnelle active et inactive

Dans le cas de l'activation/désactivation d'une directive optionnelle, il faut bien comprendre que c'est l'EAD qui prime par rapport à ERA. À la première instanciation du serveur, ERA détermine si la directive optionnelle est active ou inactive, mais une fois le serveur est instancié c'est depuis l'interface EAD qu'il faut renseigner le statut actif/inactif de la directive optionnelle en question.

Les directives optionnelles cachées

Une directive optionnelle cachée est une directive optionnelle qui n'apparaîtra pas dans l'EAD. Elle est activable uniquement par une procédure particulière.

Pour créer une directive optionnelle cachée, aller dans `Bibliothèque` / `Directives Optionnelles` et cocher `directives cachées`.



Les directives cachées

Une directive cachée est désactivée par défaut. Pour l'activer, il faut patcher le template `active_tags` afin d'y ajouter le libellé optionnel de la directive (un libellé par ligne).

Il est préférable d'utiliser un libellé optionnel court (par exemple "`ActiverProxy`" plutôt que "activer le proxy").

Dans le template `active_tags`, ne pas mettre de commentaire.

Voir aussi...

Directives optionnelles ERA depuis l'EAD [p.210]

2.2.4. La qualité de service

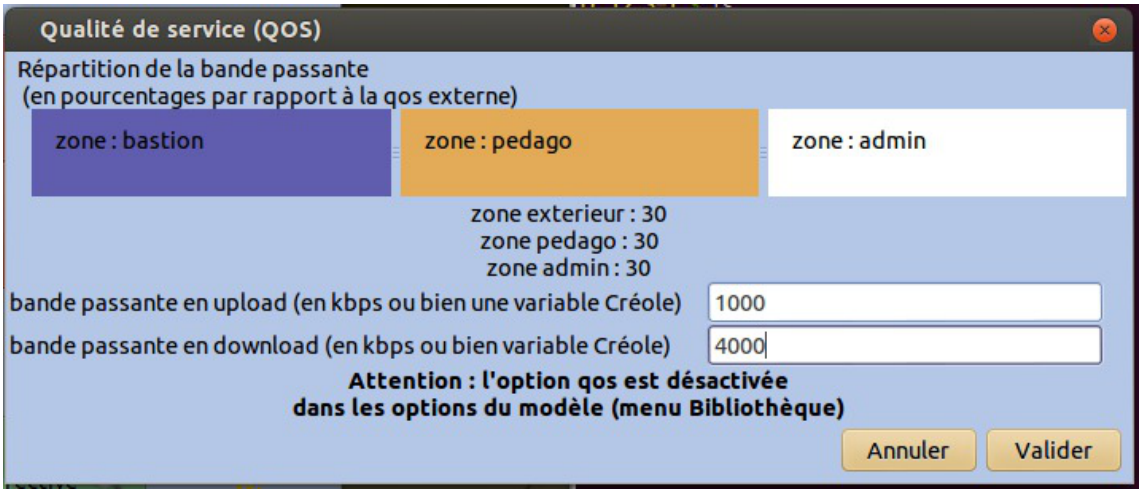
La qualité de service ne concerne que les flux des zones internes vers l'extérieur. C'est une QOS[p.312] *externe*.

Le qualité de service est un système de **minimum garanti**.

Elle n'entraîne pas de sous-utilisation de la bande passante, car si une zone n'atteint pas son minimum d'utilisation, ce qui reste est réparti dynamiquement entre les autres zones.

Il est possible d'accéder à la fenêtre de gestion de la QOS[p.312] de deux manières :

- depuis le menu `Bibliothèque` / `Qualité de service (QOS)` ;
- en cliquant sur la zone *Extérieur* depuis le tableau des flux.



Gestion de la Qualité de Service

Dans cette boîte de dialogue, il faut :

- fixer des valeurs de bande passante en *upload* et en *download* (c'est-à-dire les flux globaux disponibles entre l'intérieur et l'extérieur), en kilo bits par seconde (soit un débit de 1000 bits par seconde) ;
- à l'aide des poignées de manipulation des différentes boîtes représentant chaque zone, affecter un pourcentage de flux relatif à chaque zone.

Remarquons que il est tout-à-fait possible de mettre des variables Creole comme valeurs possibles de QOS en upload et en download

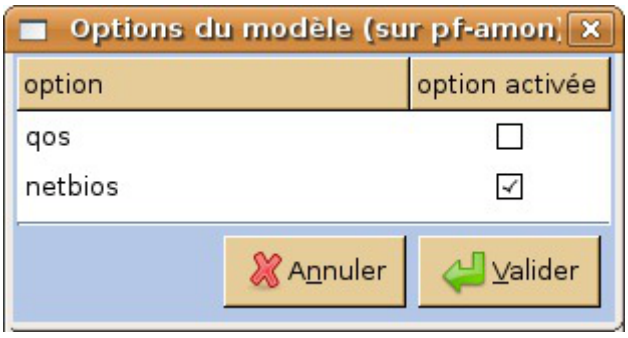
La QOS peut être définie dans un modèle sans être activée !

Pensez à l'activer dans les options du modèle (`Bibliothèque->Options du modèle`).

La désactivation de la QOS n'est effective que si le fichier `/etc/qoseole.conf` est supprimé.

2.2.5. Les options du modèle

Il est possible d'ajouter des règles spécifiques à netbios et à la QOS depuis le menu `Bibliothèque` / `Options du modèle` .



Fenêtre des options du modèle

Activer netbios permet d'ajouter des règles permettant de bloquer les requêtes du réseau Microsoft vers l'extérieur. Cette règle est activée par défaut.

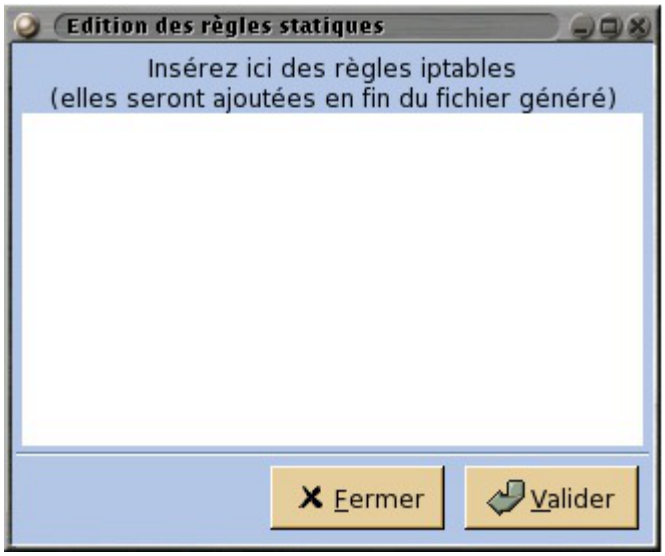
Si vous voulez utiliser les règles de Qualité de Service (QOS), il est indispensable de l'activer dans cette fenêtre. Par défaut, les règles de QOS ne sont pas actives.

2.2.6. L'inclusion statique

Il est possible d'insérer des règles iptables personnalisées. Ces règles vont venir s'insérer à la fin du fichier généré.

On accède à la fenêtre des inclusions statiques par le menu Bibliothèque / Inclusion Statique.

Il s'agit d'une zone de saisie de texte.



Fenêtre d'insertion des inclusions statiques

Aucune validation n'est faite par ERA sur ces règles insérées directement par l'utilisateur. Précisons que cette possibilité est réservée à un utilisateur avancé, qui maîtrise parfaitement la syntaxe iptables.

2.2.7. Imbriquer des modèles :l'héritage

Il est possible d'imbriquer des modèles, c'est-à-dire de faire dépendre des modèles les uns des autres. Un modèle devient un modèle père, les autres modèles héritent de toutes ses caractéristiques (directives, bibliothèques, flux, zones, ...).

Pour imbriquer des modèles, créez d'abord un modèle de manière habituelle. Ce modèle deviendra le modèle père. Ensuite, créez un nouveau fichier dans l'éditeur, et choisissez dans le menu Fichier / importer un modèle.

Le modèle est chargé comme d'habitude mais les directives importées ne sont plus éditables (elles sont grisées).

Ne seront éditables que les directives que vous allez rajouter. En plus de l'existant, vous pouvez faire

toute modification utile (ajout de zone, création de directives, etc...).

Vous ne pouvez plus changer le fichier père de place ni le renommer, le chemin du fichier père est enregistré comme attribut.

L'héritage multiple entre modèles

L'héritage d'un modèle XML est donc la possibilité de d'utiliser plusieurs fichiers XML liés entre eux par référence. Le fichier référencé dans un autre fichier est appelé le fichier père. On peut voir si on édite le fichier XML avec un éditeur de texte, que le chemin du fichier XML père est renseigné dans l'attribut **model** à la racine de la balise **firewall**.

Il est possible, mais ce n'est pas une action qui est accessible depuis l'interface gtk, d'hériter de plusieurs fichiers. Il suffit dans ce cas de mentionner dans l'attribut **model** une liste de noms longs de fichiers, séparés par des virgules. Pour des exemples de ces fonctionnalités, regarder dans le dossier **template** dans les sources du projet ERA, car les modèles XML eux-mêmes sont générés à partir de templates qui sont imbriqués entre eux avec cette fonctionnalités de l'héritage multiple.

2.2.8. Communication avec Zéphir

La connexion au Zéphir est possible depuis le menu `Zephir`.

Connection à Zéphir

Importer un modèle

ERA intègre la possibilité d'échanger des modèles avec un serveur Zéphir.

Lors du première utilisation des fonctions d'importation Zéphir, des informations de connexion vous seront demandées.

Vous devez spécifier ici l'adresse du serveur Zéphir, et le nom et le mot de passe d'un utilisateur ayant les droits nécessaires (lecture pour l'import et écriture pour l'export). Une fois connecté, vous pourrez saisir l'identifiant du serveur.

Le modèle est alors téléchargé et ouvert dans ERA. Cette procédure n'est valable que si vous avez déjà remonté le modèle de pare-feu dans Zéphir.

Importation d'un modèle XML depuis le Zéphir

A l'enregistrement, il vous sera demandé si vous voulez remonter le modèle sur Zéphir.

Exporter un modèle Zéphir

Lorsque vous avez construit un modèle de pare-feu, vous pouvez l'envoyer directement sur un serveur Zéphir avec le menu `Envoi à zephir`. Si vous ne les avez pas encore renseignées, ERA vous demandera les informations nécessaires à la connexion.

Les options suivantes vous sont proposées pour la sauvegarde sur Zéphir :

- pour un serveur : sauvegarde le modèle sur le serveur et change le modèle actif dans la configuration du serveur ;
- pour une variante : le fichier est ajouté à la liste des fichiers de la variante ;
- pour un groupe : idem que pour un seul serveur, mais sur tous les Amon présents dans le groupe choisi.

Exportation vers Zéphir

2.3. Directives optionnelles ERA depuis l'EAD

Les modèles de pare-feu ERA peuvent contenir des directives optionnelles[p.304].

Une règle peut être :

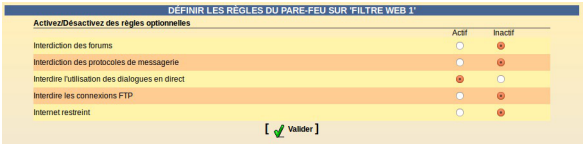
- générale, si elle concerne l'interface externe ;
- spécifique à une zone de configuration, si elle concerne une interface interne de la zone.

La configuration générale est accessible par le menu EAD : `Configuration générale` / `Règles du pare-feu`.

La configuration spécifique est accessible par le menu EAD : `Filtre web X` / `Règles du pare-feu` :

Pour valider une directive optionnelle :

- choisir Actif ;
- valider.



L'interface graphique d'ERA

Lien entre ERA et les directives optionnelles de l'EAD

Pour les règles optionnelles, l'EAD prime sur l'ERA : elles sont pilotées par l'EAD. Une directive peut être marquée comme étant active par défaut dans ERA et ne pas être active car désactivée dans l'interface EAD.

Voir aussi...

Les directives optionnelles [p.255]

2.4. Exceptions sur la source ou la destination

Par défaut, tous les accès à des sites nécessitent une authentification (si elle est active) et toutes les machines du réseau doivent s'identifier. Mais certains systèmes ou logiciels doivent pouvoir se mettre à jour de façon transparente.

Par ailleurs, le proxy conserve une version des pages téléchargées en cache pour limiter la consommation réseau. Ce comportement n'est pas adapté à tous les sites.

Pour les sites comportant des données sensibles, il est nécessaire de s'assurer que des données relatives à la navigation sur ce domaine ne soient pas placées dans le cache du serveur.

Certaines machines peuvent également avoir besoin de naviguer avec des données provenant directement du site consulté.

Certains postes clients ou serveurs du réseau ont besoin d'effectuer des mises à jour automatiquement, les sites de mise à jour doivent être accessibles sans authentification.

Certaines machines peuvent également avoir besoin de naviguer sans être authentifiées.

Pour cela, il existe deux mécanismes :

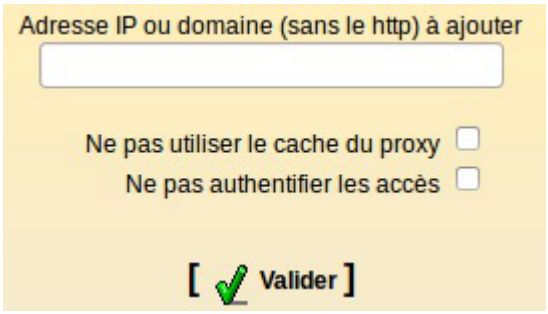
- ne pas utiliser de cache ou d'authentification pour certains sites (destination) ;
- ne pas utiliser de cache ou d'authentification pour certaines machines locales (source).

Pour paramétrer les destinations et les sources qui n'utiliseront pas le cache ou l'authentification lors de la navigation il faut se rendre dans `Configuration générale` puis `Cache et Authentification` de l'interface EAD du module.

Cache et authentification de la destination

Dans `Configuration générale` / `Cache et Authentification` / `Destinations` :

- entrer l'adresse IP ou le nom du domaine ;
- cocher authentification et/ou cache ;
- valider.



Ajout d'une destination à ne pas authentifier et/ou pour laquelle ne pas utiliser le cache

Pour supprimer une référence, cliquer sur la croix rouge correspondante :

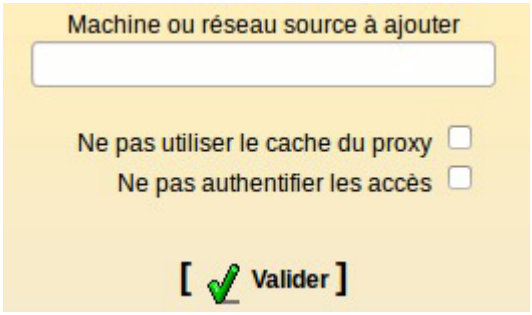
Destination	Cache	Authentification
10.121.58.5	✗	✗
ac-dijon.fr	✗	✗
scribe		✗

Listes des destinations à ne pas authentifier et/ou pour lesquelles ne pas utiliser le cache

Cache et authentification de la source

Dans `Configuration Générale` / `Cache et Authentification` / `Sources` :

- entrer l'adresse IP ou réseau
- cocher authentification et/ou cache ;
- valider.



Ajout d'une source à ne pas authentifier et/ou pour laquelle ne pas utiliser le cache

Pour supprimer une référence, cliquer sur la croix rouge correspondante :

Source	Cache	Authentification
10.121.58.5	✗	✗
10.21.58.10	✗	✗
172.16.0.0/24		✗
172.16.0.6	✗	✗

Listes des sources à ne pas authentifier et/ou pour lesquelles ne pas utiliser le cache

Personnalisations académiques

Des listes de sites et d'adresses académiques peuvent être gérées indépendamment de l'EAD par l'intermédiaire des fichiers suivants :

- `/etc/squid3/domaines_noauth_acad` : liste de destinations à ne pas authentifier ;
- `/etc/squid3/domaines_nocache_acad` : liste de destinations pour lesquelles ne pas utiliser le cache ;

- `/etc/squid3/src_noauth_acad` : liste de sources à ne pas authentifier ;
- `/etc/squid3/src_nocache_acad` : liste de sources pour lesquelles ne pas utiliser le cache ;
- `/etc/squid3/domaines_nopeerproxy` : liste de destinations pour lesquelles on n'utilise pas le proxy père.

2.5. Compléments techniques

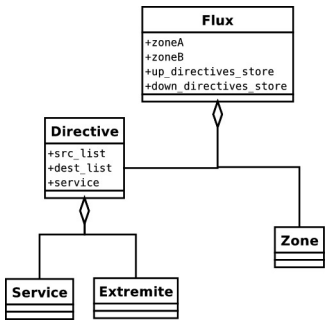
2.5.1. Le format XML interne

Les composantes du tableau des flux sont :

- les flux ;
- les zones ;
- les directives montantes et descendantes.

Le format XML interne suit une DTD qui correspond à la modélisation par flux. Les noms des balises correspondent aux noms des objets ERA. Il y a la liste des zones, puis les extrémités et les services, les groupes de services, et enfin les flux contenant les directives.

La représentation interne en objets est la suivante :



La représentation interne (objets)

- Directive(FwObject) : directive ;
- Service(FwObject), ServiceGroupe(FwObject) : service et liste de services ;
- Zone(FwObject), Extremite(FwObject) ;
- Flux(FwObject).

Les directives optionnelles

Dans le fichier `era.noyau.constants.py` il y a deux constantes intéressantes ici

- `DIRECTIVE_OPTIONAL = 1`
- `DIRECTIVE_ACTIVE = 2`

Ces filtres permettent de savoir si une directive est optionnelle ou non. Pour cela, il faut regarder l'attribut `attrs` de la directive.

Si `directive.attrs = 0`, alors la directive n'est ni optionnelle, ni active.

- `attrs=0` : pas optionnelle

- `attrs=1` : optionnelle mais pas active
- `attrs=3` : optionnelle et active
- la valeur 2 correspond à non optionnelle mais active, ce qui n'a pas de sens. Les valeurs autorisées sont donc `[0,1,3]`
- `ACTION_DENY` = 1 : barrage
- `ACTION_ALLOW` = 2 : pont
- `ACTION_FORWARD` = 4 : redirect
- `ACTION_DNAT` = 8 : dnat
- `ACTION_MASK` = 16 : masque

Exemple d'une directive de type masque :

```
action="16" attrs="0" nat_extr="exterieur_bastion" nat_port="0"
```

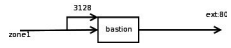
Exemple d'une directive de type dnat :

```
action="8" attrs="0" nat_extr="serveur_web" nat_port="80"
```

2.5.2. Comportement du Backend

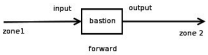
Règles implicites : le REDIRECT

Un redirect doit inclure aussi une chaine input chaine xxx-bas. A une règle de forward vient donc se greffer une règle de type input.



règles implicites : le redirect

Il y a une règle de forward (une redirection) :



La règle de forward

la chaine input qui vient se greffer sur le redirect (sur le forward) est implicite.un forward z1->z2 doublé d'une redirection, ajoute une règle de type input vers le bastion.

Une directive de redirection génère donc deux règles :

- une règle input vers le bastion
- une règle forward z1->z2

La règle dite "implicite" est la règle de type INPUT. Une règle implicite se place en fin de pile pour chaque flux (elle n'est pas placée directement à côté de sa règle de FORWARD dans le fichier de règles générées).

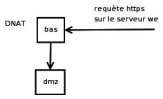
Règles implicites : Le DNAT et le SNAT

Lors d'un DNAT, une règle de type input est doublée d'un forward (elle s'ajoute à un FORWARD).

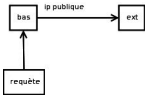
Même chose pour le masque de SNAT.

Exemple : un serveur de la DMZ répond à une requête sur le port 80 du bastion.

Un INPUT est transformé en FORWARD.



requête de DNAT



Une règle de type SNAT

Un poste de travail peut surfer sur le web avec l'IP publique du bastion. Cela permet de surfer masqué.

2.5.3. Intégration avec Creole

Creole propose un concept de variables multivaluées qui peuvent être utilisées dans ERA. ERA utilise bien-sûr les variables de dictionnaire Creole "simples", mais la fonctionnalité d'utilisation des variables de dictionnaires dans ERA peut-être étendue aux fonctionnalité Creole.

Si une variable `%%variable` est multi-valuée (au sens de Creole, c'est-à-dire que ça peut-être une liste), et que cette variable est présente dans une règle iptables, alors la règle iptables sera répétée autant de fois que de valeurs dans `%%variable` cette fonctionnalité génère du code avec une boucle for :

`%for %%v in %%variable` `/sbin/iptable bla bla %%v bla bla` `%end for`

2.5.4. Le compilateur

La génération des règles iptables

A la compilation du fichier XML, un certain nombre d'actions sont effectuées. Ce sont des règles iptables :

- définition d'une sous-chaîne pour chaque flux (liaison entre zone/extrémité) ;
- création de la politique par défaut (en fonction du niveau des zones) ;
- ajout des règles correspondant aux directives ;
- ajout de règles implicites liées au directives ;
- insertion des inclusions statiques (règle iptables de bas niveau).

Sur Amon, le compilateur gère aussi l'affichage des règles optionnelles dans l'EAD et récupère leur configuration en cas de mise à jour, et contrôle l'activation des directives cachées.

Le script iptables peut-être généré depuis l'interface ERA ou bien depuis un utilitaire ligne de commande plus complet.

Le bouton `générer`, bouton de génération des règles iptables n'est utile que si l'on n'est pas sur un Amon.

Il est donc possible depuis l'interface de transcrire directement en règles iptables ce qui est enregistré dans le fichier XML.

Bouton de génération de la sortie au format iptables

C'est aussi au moment de la compilation que sont gérées les directives cachées. Elles sont activées ou désactivées selon ce qui a été spécifié.

Utilisation en ligne de commande

Aller dans le répertoire era `/usr/share/era` et lancer le compilateur avec le fichier de modèles adapté

[era] `$ ./backend/compiler --help`

`compiler [options] era_model_file.xml`

par exemple :

[era] `$ ./backend/compiler modeles/3zones.xml`

différentes options sont possibles, taper `--help` pour les détails ou regarder le fichier `/usr/share/era/bastion.sh` qui correspond à ce qui est lancé par le service **bastion**

`service bastion restart` est lancé

2.6. Quelques références

- Site officiel du logiciel (présentation, téléchargement) : http://eole.orion.education.fr
- Code source du logiciel (versions, branches, tags) : https://dev-eole.ac-dijon.fr/projects/era/repository

3. Gestion des tunnels : RVP

Pré-requis

Le réseau virtuel privé (RVP)[p.312] est activé au moment de la configuration et de l'instanciation du module.

Sur le module Amon, il faut au préalable avoir activé et configuré le réseau virtuel privé dans l'interface de configuration du module. Sur le module Sphynx, ce paramètre est forcé et n'apparaît pas.

Le mode de configuration de strongSwan (database ou fichier plat) doit être le même que sur le serveur ARV qui a généré la configuration IPsec.

ARV[p.301] permet de gérer les RVP de plusieurs serveurs Sphynx. Un serveur Sphynx autre que le serveur Sphynx-ARV sera appelé Sphynx distant. Sur un serveur de ce type, la mise en place du RVP se fera comme sur un serveur Amon.

Activation du RVP au moment de l'installation du serveur Amon

La configuration du Réseau Virtuel Privé peut se faire avec un serveur Zéphir ou manuellement.

Dans le cas d'une configuration manuelle il faut préparer la configuration avant l'instanciation :

- copier le répertoire /home/data/vpn/<UAI>/<UAI>-amon.tar.gz présent sur le module Sphynx sur le module Amon dans /tmp/sphynx.tar.gz ;
- sur le module Amon créer le répertoire ConfIpsec : `# mkdir -p /root/tmp/ConfIpsec` ;
- se rendre dans le répertoire /root/tmp/ConfIpsec : `# cd /root/tmp/ConfIpsec` ;
- désarchiver sphynx.tar.gz : # tar xzf /tmp/sphynx.tar.gz

Au lancement de la première instanciation, la question suivante vous sera posée :

`Voulez-vous configurer le Réseau Virtuel Privé maintenant ? [oui/non] [non] :`

Vous devez répondre `oui` à cette question.

Puis le choix 1.Manuel ou 2.Zéphir est proposé.

- Le choix 1.Manuel permet de prendre en compte la configuration RVP présente sur le serveur, attention cette opération doit être effectuée avant d'exécuter l'instanciation ;
- Le choix 2.Zéphir active la configuration RVP présente sur le serveur Zéphir. Cela suppose que le serveur est déjà enregistré sur le serveur Zéphir. Il sera demandé un utilisateur et mot de passe Zéphir et l'identifiant Zéphir du serveur Sphynx.

Dans les deux cas, la phrase de passe (passphrase) de la clé privée est demandée. Si le mot de passe est correct le RVP est configuré pour cette machine et l'instanciation peut se poursuivre...

Activation du RVP sur des modules Amon déjà en exploitation

Pour activer un RVP sur un module Amon déjà instancié, il faut lancer en tant qu'utilisateur `root` la commande `active_rvp init`.

Suppression du RVP

Pour supprimer un RVP, il faut lancer en tant qu'utilisateur `root` la commande `active_rvp delete`.

Chapitre 7

Paramétrage des postes client

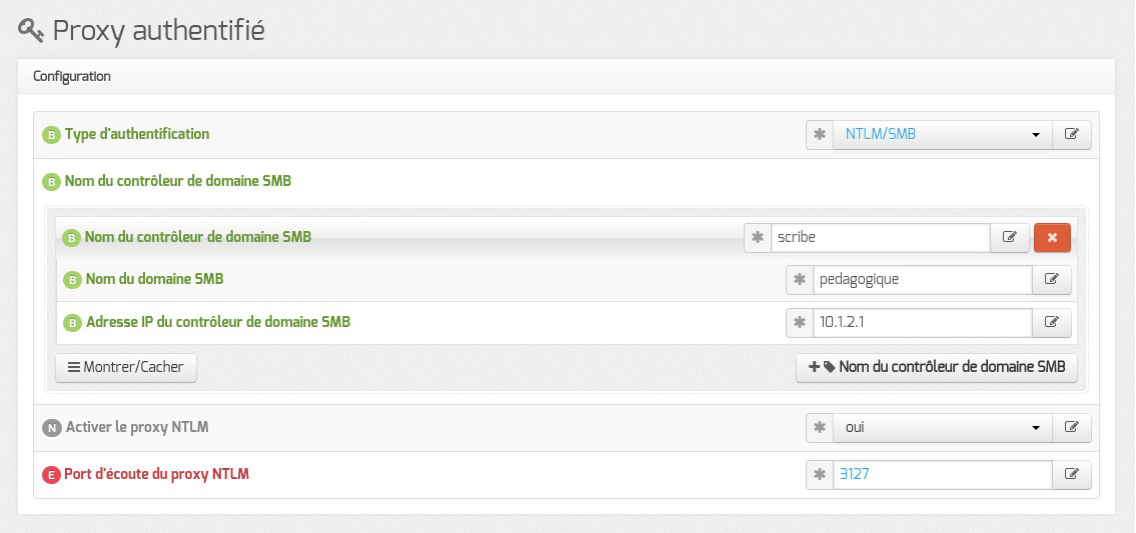
1. Authentification NTLM/SMB - NTLM/KERBEROS hors domaine

L'authentification NTLM[p.309] pour des postes hors domaine est facilité par l'utilisation du proxy Cntlm[p.303].

Installation et activation

Cntlm est pré-installé sur les modules Amon, AmonEcole et ses variantes.

L'activation du service se fait dans l'interface de configuration du module dans l'onglet `Proxy authentifié`. Cet onglet n'est disponible que si l'authentification web a été, elle-même, activée dans l'onglet `Authentification`.



Vue de l'onglet Proxy authentifié dans l'interface de configuration du module

Il faut choisir le type d'authentification sur le proxy `NTLM/SMB` ou `NTLM/KERBEROS`.

Ensuite il faut passer la variable `Activer le proxy NTLM` à `oui`.

Par défaut, le port de Cntlm est le `3127` mais sa valeur peut être modifiée par le biais de la variable experte intitulée : `Port d'écoute du proxy NTLM`.

L'activation du service est effective après une reconfiguration du serveur avec la commande :

```
# reconfigure
```

Attention, si l'authentification de type `NTLM/SMB` est choisie, c'est le premier domaine spécifié qui sera utilisé par Cntlm.

Configuration des clients hors domaine

L'authentification proxy NTLM/SMB et NTLM/KERBEROS nécessite une configuration particulière des postes clients Windows.

Par défaut, il est nécessaire, par exemple, de modifier la base de registre sur le poste Windows Seven.

Mais dans le cas de l'utilisation de Cntlm aucun changement n'est requis dans la base de registre pour les postes hors domaine.

Les postes nomades (hors domaine) doivent utiliser le port `3127` pour passer par Cntlm.

Configuration des clients du domaine

Pour continuer à profiter de l'authentification transparente, les postes intégrés au domaine ne doivent pas passer par Cntlm.

Il est donc nécessaire de configurer correctement les postes du domaine avec, par exemple, ESU[p.305].

Les postes intégrés au domaine doivent donc utiliser le port `3128` pour passer par le proxy .

Dans le cas où la découverte automatique du proxy avec WPAD est activée, le port proposé par défaut est automatiquement celui du proxy NTLM Cntlm (`3127` par défaut).

Voir aussi...

Configurer la découverte automatique du proxy avec WPAD [p.197]

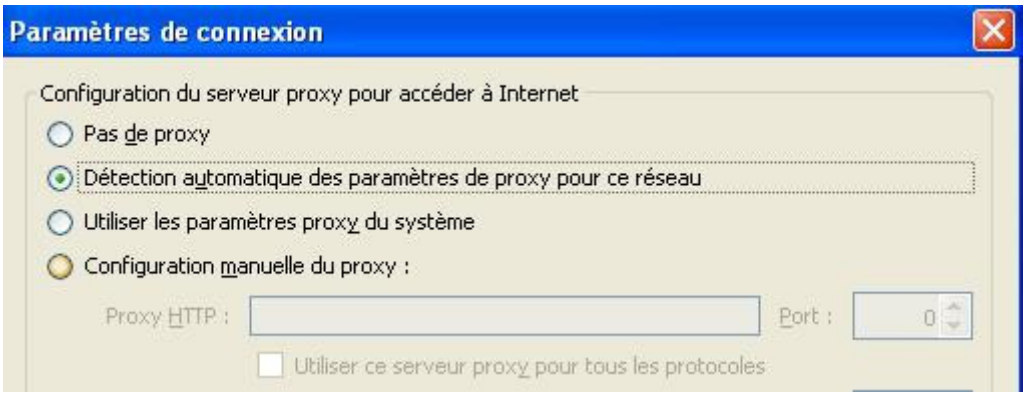
Onglet Proxy authentifié : 5 méthodes d'authentification [p.74]

2. Configurer la découverte automatique du proxy avec WPAD

WPAD[p.314] est un protocole qui permet la découverte automatique du proxy par les navigateurs.

Le principe est simple, si le navigateur est configuré pour détecter automatiquement la configuration du proxy, il essayera de télécharger le fichier : `wpad.<domaine local>/wpad.dat` ou le fichier `proxy.pac`.

Configuration côté client



Détection automatique du proxy dans Firefox

Par défaut, les adresses pour lesquelles le proxy ne sera pas utilisé sont : 127.0.0.1 et le réseau local.

La détection automatique du proxy par les navigateurs peut être imposée par des outils tels que :

- ESU/client Scribe ;
- Gaspacho.

Dans le cas de l'activation du proxy Cntlm[p.303] le numéro de port change mais sa prise en charge est automatisée, il n'y a donc rien à faire.

Configuration côté serveur

Pour fonctionner correctement, WPAD a besoin de trois éléments qui sont pris en charge par EOLE :

- un serveur web qui diffuse le fichier, dans le cadre d'EOLE, c'est le service Nginx[p.308] qui se charge de distribuer les fichiers `wpad.dat` adaptés à chacun des sous-réseaux.
- un nom de domaine `wpad.<nom_domain_local>` qui pointe vers le serveur web ;
- un serveur DHCP configuré pour envoyer le chemin du fichier.

Par défaut, la configuration est correctement définie sur un AmonEcole mais dans le cadre d'un environnement Amon / Scribe ou Amon / Horus il faut configurer correctement les deux modules.

Configuration sur le module Scribe

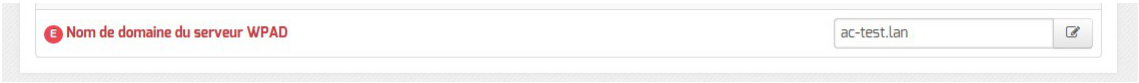
Le serveur DHCP doit être activé et correctement configuré sur le module Scribe.

Dans l'interface de configuration du module en mode expert, dans l'onglet `Dhcp`, le champ `Nom de domaine du serveur WPAD` permet de configurer le nom de domaine du serveur WPAD.

Même s'il est possible d'utiliser n'importe quel domaine, il est conseillé d'utiliser la même valeur que celle utilisée pour le nom de domaine local.

Pour les postes de travail Windows c'est la valeur du champ `Nom de domaine du serveur WPAD` qui sera utiliser pour accéder au fichier WPAD tandis que pour des postes

> de travail GNU/Linux c'est le nom de domaine local qui sera utilisé pour accéder au fichier WPAD.



Vue de l'onglet Dhcp de l'interface de configuration du module

Dans l'interface de configuration du module, en mode expert, il faut saisir dans le `Nom de domaine du serveur WPAD` de l'onglet `Dhcp` la même valeur que celle du champ `Nom de domaine privé du réseau local` de l'onglet `Général`.

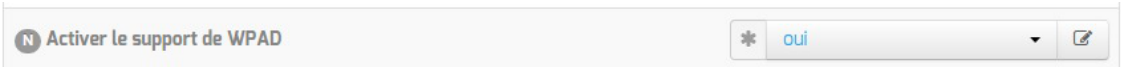
> Pour être pris en compte, les changements doivent être enregistrés et suivis de la commande `reconfigure` sur le module.

Configuration sur le module Amon

WPAD est mise à disposition sur les modules Amon et ses variantes (AmonEcole, ...) au travers du paquet `eole-wpad` mais n'est fonctionnel que si le paquet `eole-proxy` est installé.

Pour fonctionner correctement, il faut que l'URL `wpad.<nom_domaine_local>` correspondre à l'adresse IP du serveur web.

Le support de WPAD doit être activé et correctement configuré sur le module Amon.



Activation de WPAD dans l'onglet Services

Dans l'onglet `Services` de l'interface de configuration du module `Activer le support de WPAD` doit être placé à `oui`.

Vue de l'onglet Wpad dans l'interface de configuration du module

Cela rend disponible l'onglet `Wpad` au sein duquel le `Nom de domaine du service WPAD` doit être rempli avec la même valeur que le `Nom de domaine privé du réseau local` présent dans l'onglet `Général`.

> Si vous souhaitez utiliser un autre nom de domaine qui ne correspondrait pas au `Nom de domaine privé du réseau local` de l'onglet `Général`, il faut le déclarer dans le champ `Nom domaine local supplémentaire ou rien` de l'onglet `Zones-dns`.

Pour être pris en compte, les changements doivent être enregistrés et suivis de la commande `reconfigure` sur le module.

WPAD supporte les VLAN et les alias, Nginx renvoie le bon fichier WPAD si des VLAN ou des alias sont déclarés.

En mode expert, Il est également possible de changer le port du proxy diffusé par défaut pour une interface, un VLAN ou un alias donné.

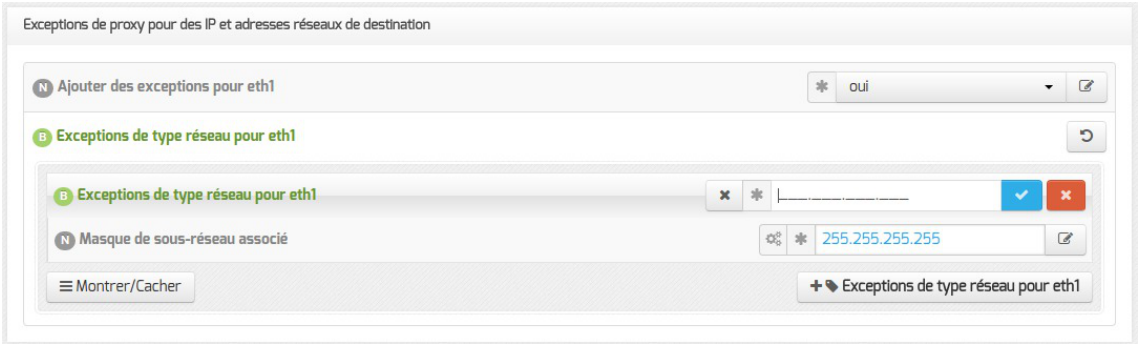
Ajouter des exclusions dans la configuration automatique du proxy

Dans l'onglet `Exceptions proxy` de l'interface de configuration du module il est possible d'ajouter des exclusions dans la configuration automatique du proxy.

Il est possible de déclarer différents types d'exceptions.

Exception sur une adresse IP ou une plage d'adresses IP

Cette exception commune à ERA et à WPAD permet de déclarer une adresse IP ou une plage d'adresses IP de destination pour laquelle on ne passe pas par le proxy.



Le bouton `Exceptions de type réseau pour eth-n` permet d'ajouter plusieurs exceptions sur une même interface.

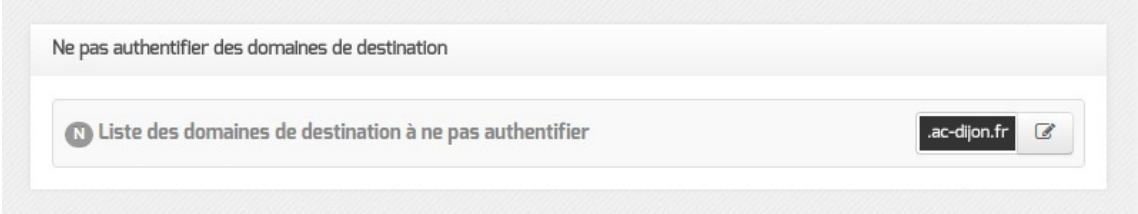
Exception sur un nom de domaine

Cette exception commune à ERA et à WPAD permet de déclarer un domaine de destination pour lequelle on ne passe pas par le proxy.

Il est possible d'ajouter plusieurs exceptions sur une même interface.

Exception au niveau de l'authentification des domaines

Cette exception permet de déclarer des sites pour lesquels le proxy ne demandera pas l'authentification à l'utilisateur qui souhaite y accéder.



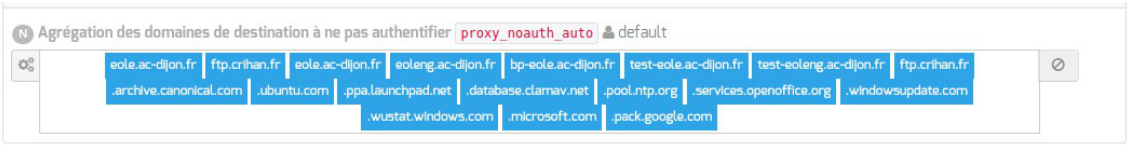
Si cNTLM et WPAD sur activés sur l'interface réseau, les utilisateurs utiliseront directement Squid (sans passer par cNTLM) pour accéder à ces sites.

Les domaines commençants par un `.` sont gérés, le domaine lui-même et les sous-domaines ne sont pas authentifiés.

Si on spécifie la valeur `.ac-dijon.fr` alors `ac-dijon.fr` et `www.ac-dijon.fr` seront autorisés sans authentification.

Une liste de sites à ne pas authentifier par défaut est stockée dans la variable cachée `proxy_noauth_auto`.

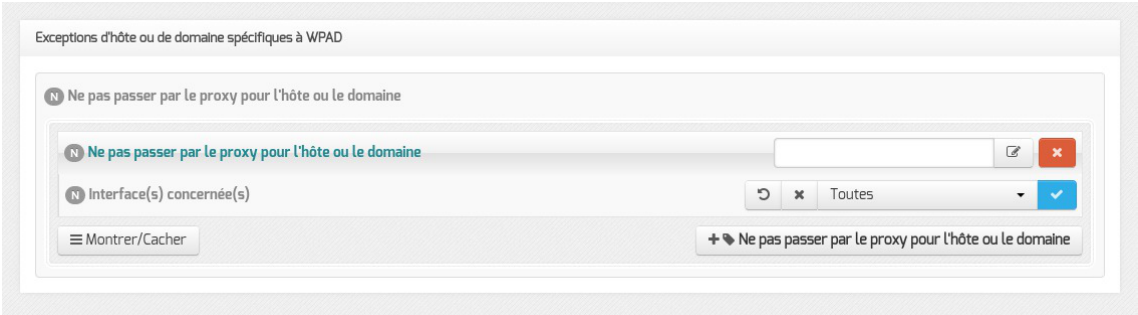
Il est possible de l'afficher dans l'onglet Exceptions proxy de l'interface de configuration du module en activant le mode Debug.



Cette variable reprend la liste des sites qui étaient dans le template domaines_noauth des versions EOLE antérieures à 2.5.2.

Exception sur un nom d'hôte (spécifique à WPAD)

L'exception sur un nom d'hôte s'effectue sur le nom d'hôte et sur le nom d'hôte complet.



Il faut choisir une interface ou toutes les interfaces sur lesquelles l'exception sera appliquée. Le bouton + Ne pas passer par le proxy pour l'hôte ou le domaine permet d'ajouter plusieurs exceptions sur une même interface.

Ce type d'exception étant spécifique à WPAD, il n'est pas prise en compte par les autres services gérant des exceptions au niveau du proxy.

Si le champ `Ne pas passer par le proxy pour l'hôte ou le domaine` a comme valeur `www.ac-monacad.fr`, le fichier WPAD.dat généré contiendra la ligne `|| localHostOrDomainIs(host, "www.ac-monacad.fr")` qui permet d'exclure simplement des URLs.

Compléments sur `Ne pas passer par le proxy pour le` domaine (dnsDomainIs) :

http://findproxyforurl.com/netscape-documentation/#dnsDomainIs

Compléments sur `Ne pas passer par le proxy pour l'hôte ou le domaine` (localHostOrDomainIs) :

http://findproxyforurl.com/netscape-documentation/#localHostOrDomainIs

Configuration du serveur DHCP sur le module Scribe

Onglet Dhcp : Configuration du serveur DHCP

3. Proxy non configuré dans le navigateur : redirection ou page d'information

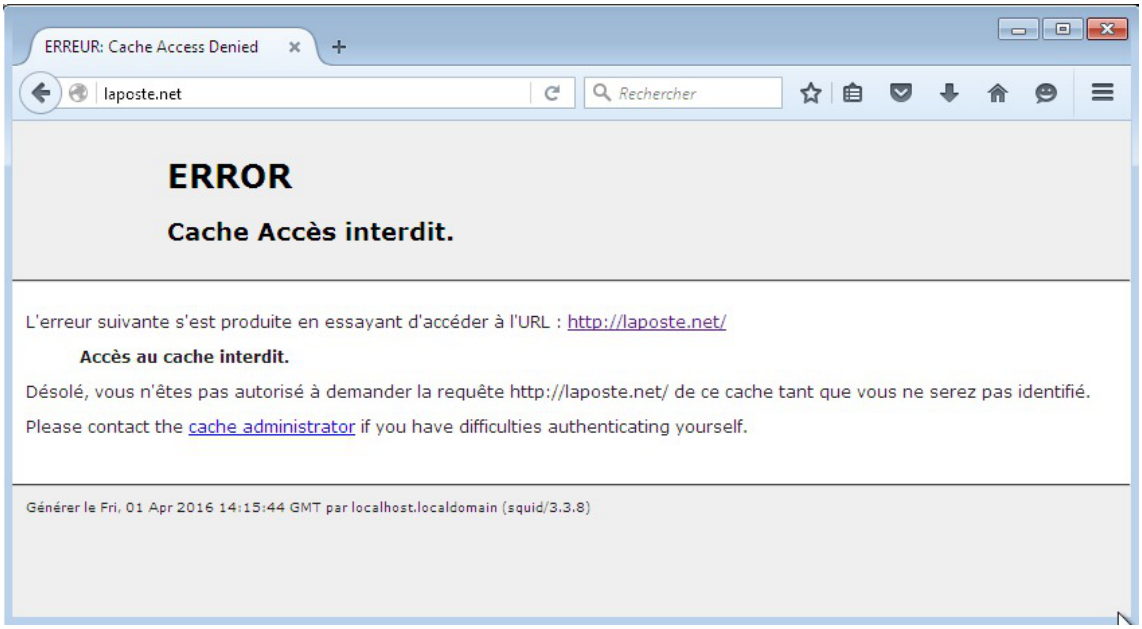
Redirection transparente HTTP sur Amon

Sur le module Amon, les flux HTTP provenant des réseaux internes sont redirigés vers le proxy.

La redirection transparente ne fonctionne pas avec le protocole HTTPS car il s'agit d'un mode connecté qui ne supporte pas ce genre de manipulation sur les paquets. La redirection est faite uniquement pour obliger les postes à utiliser le proxy.

La redirection transparente n'est pas mise en place sur le module AmonEcole et ses variantes.

Si l'authentification du proxy est activée sur l'interface, la redirection fonctionnera mais pas l'authentification et l'utilisateur obtiendra une page d'erreur explicite provenant du logiciel Squid.



Page d'erreur renvoyée par Squid en cas d'erreur d'authentification

Dans l'onglet `Exceptions proxy` de l'interface de configuration du module, il est possible de déclarer des adresses de destination qui seront exclues de la redirection vers le proxy.

Page d'information renvoyée par Nginx

Sur les modules Amon et AmonEcole, la configuration du logiciel Nginx a été adaptée afin de détecter le cas où le navigateur du client n'a pas été configuré correctement et lui renvoyer un message d'erreur suffisamment explicite.

Page d'erreur renvoyée par Nginx en cas de proxy non configuré

La page d'erreur affichée dans le navigateur peut être personnalisée.

Personnaliser la page renvoyée par Nginx à l'aide d'un patch

La page d'erreur affichée dans le navigateur est un template Creole : `/usr/share/eole/creole/distrib/nginx.no_proxy.html`

Il est possible de le modifier de façon pérenne en utilisant un patch pour Creole.

Il faut copier le template d'origine dans le répertoire `/usr/share/eole/creole/modif/`

```
root@amon:~# cp /usr/share/eole/creole/distrib/nginx.no_proxy.html /usr/share/eole/creole/modif/nginx.no_proxy.html
```

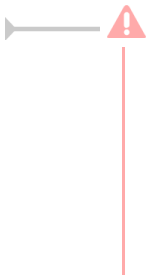
Il faut éditer, modifier et enregistrer le fichier copié

```
root@amon:~# vim /usr/share/eole/creole/modif/nginx.no_proxy.html
```

Puis il faut générer le patch à l'aide de la commande `gen_patch`

```
root@amon:~# gen_patch
```

Le fichier contenant les différences est créé dans le répertoire `/usr/share/eole/creole/patch/`

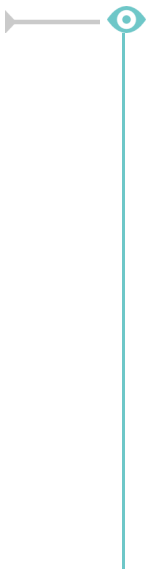


Les changements prennent effet après la reconfiguration du serveur à l'aide de la commande reconfigure

```
root@amon:~# reconfigure
```

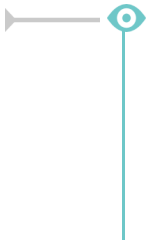
La page servie par Nginx contient les modifications :

```
root@amon:~# vim /var/www/index.html
```



```
root@amon:~# cp /usr/share/eole/creole/distrib/nginx.no_proxy.html
/usr/share/eole/creole/modif/nginx.no_proxy.html
root@amon:~# vim /usr/share/eole/creole/modif/nginx.no_proxy.html
[...]
root@amon:~# gen_patch

** Génération des patches à partir de modif **

Génération du patch nginx.no_proxy.html.patch

** Fin de la génération des patch **

root@amon:~# ls /usr/share/eole/creole/patch/
nginx.no_proxy.html.patch  variante
root@amon:~# reconfigure
[...]
root@amon:~# vim /var/www/index.html
```

Il est possible d'appeler des variables Creole comme par exemple `%%libelle_etab` et aussi d'ajouter des images en les ajoutant par exemple dans un dossier `/img` dans `/var/www/`.



```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN"
"http://www.w3.org/TR/html4/strict.dtd">
<html>
    <META http-equiv="Content-Type" content="text/html; charset=utf-8;">
    <head>
<title>Veuillez configurer le proxy de votre navigateur</title>
```

```
<style>
.main {
        background:#bbbbbb;
        text-align:center;
}
h1 {
    /* text-shadow: 0px 0px 7px rgba(0, 0, 0, 0.75);*/
    color: #91e842;
    font-size: 50px;
    text-align:center;
    text-shadow: 0 1px 0 #eee,
              0 2px 0 #e5e5e5,
              -1px 3px 0 #C8C8C8,
              -1px 4px 0 #C1C1C1,
              -2px 5px 0 #B9B9B9,
              -2px 6px 0 #B2B2B2,
              -2px 7px 2px rgba(0,0,0, 0.6),
              -2px 7px 8px rgba(0,0,0, 0.2),
              -2px 7px 45px rgba(0,0,0, 0.4);
}
.message {
    top:25%;
    text-align:center;
    margin-left: 50px;
    margin-right: 50px;

    padding: 40px;
    background: #d2ff52;
    border: 1px solid #000000;

    border-radius: 10px;
    -moz-border-radius: 10px;
    -webkit-border-radius: 10px;

    box-shadow: 5px 7px 10px 6px rgba(119, 119, 119, 0.75);
    -moz-box-shadow: 5px 7px 10px 6px rgba(119, 119, 119, 0.75);
    -webkit-box-shadow: 5px 7px 10px 6px rgba(119, 119, 119, 0.75);
}
</style>
    </head>
    <body class='main'>
    <img src="./img/logoEolePt.png">
    <h1>%%libelle_etab</h1>
    <h2>Votre navigateur n'est pas correctement configuré !!</h2>
    <div class="message">Pour naviguer sur internet, un proxy doit être
déclaré dans votre navigateur.<br />
Si vous accédez à la présente page, c'est que votre navigateur n'est pas
configuré pour utiliser le proxy. Veuillez contacter le service informatique
de l'établissement.</div>
    </body>
</html>

```

Page d'erreur renvoyée par Nginx en cas de proxy non configuré

4. Synthèse des paramètres proxy à utiliser pour les postes client

Module Amon standard

Sur une installation standard du module Amon, l'adresse du proxy sera l'adresse du serveur Amon sur le réseau. Le port sera celui de e2guardian (3128 par défaut), ce qui donne par exemple :

- proxy sur le réseau administratif : `adresse_ip_eth1:3128`
- proxy sur le réseau pédagogique : `adresse_ip_eth2:3128`
- proxy sur la DMZ : `adresse_ip_eth3:3128`

Module AmonEcole et ses variantes

Sur une installation standard des modules AmonEcole/AmonHorus, l'adresse du proxy sera l'adresse IP réservée pour le proxy sur le réseau. Le port sera celui de e2guardian (3128 par défaut), ce qui donne par exemple :

- proxy sur le réseau AmonEcole : `adresse_ip_eth1_proxy_link:3128`

On notera que, comme sur un module Amon standard, la passerelle est l'adresse du module Amon sur le réseau (adresse_ip_eth1). Mais par contre pour le DNS, il faut utiliser la même adresse IP que celle du proxy.

Double authentification

Si la double authentification est configurée, le port à utiliser pour le second proxy sera celui de la troisième configuration e2guardian (variable `dansguardian_port3` : 3129 par défaut), soit :

- proxy2 sur le réseau eth1 Amon : `adresse_ip_eth1:3129`
- proxy2 sur le réseau AmonEcole : `adresse_ip_eth1_proxy_link:3129`

Proxy NTLM

Si l'authentification NTLM pour des postes hors domaine est configurée :

- les postes intégrés au domaine doivent continuer à utiliser le port de e2guardian (3128 par défaut) ;
- les postes nomades (hors domaine) doivent utiliser le port défini par la variable `cntlm_port` (3127 par défaut) pour passer par Cntlm.

Filtrage web désactivé

Si le filtrage web est désactivé, le proxy Squid écoute sur le port 3128 en lieu et place du logiciel de filtrage e2guardian.

En cas de double authentification, le second proxy répondra sur le port 3129.

Chapitre 8

Compléments techniques

Cette partie de la documentation regroupe différentes informations complémentaires : des schémas, des informations sur les services, les ports utilisés sur chacun des modules...

1. Les services utilisés sur le module Amon

Les services disponibles sur les modules EOLE ont été répartis dans des paquets distincts, ce qui rend leur installation complétement indépendante.

Un module EOLE peut donc être considéré comme un ensemble de services choisis et adaptés à des usages précis.

Des services peuvent être ajoutés sur les modules existants (exemple : installation du paquet `eole-dhcp` sur le module Amon) et il est également possible de fabriquer un module entièrement personnalisé en installant les services souhaités sur une installation Eolebase.

1.1. eole-antivirus

Le paquet `eole-antivirus` permet la mise en place d'un serveur antivirus.

Ne pas confondre ce paquet avec `eole-antivir` qui permet la mise en place de la gestion d'un antivirus centralisé de type OfficeScan de Trend Micro.

http://dev-eole.ac-dijon.fr/projects/eole-antivir

http://eole.ac-dijon.fr/presentations/2011%20novembre/eole-antivir.pdf

Logiciels et services

Le paquet `eole-antivirus` s'appuie sur les services clamav-daemon [http://www.clamav.net/] et clamav-freshclam.

Historique

A la base, les services clamav et freshclam étaient déjà sur la plupart des modules afin de servir à d'autres services tels que le serveur de fichiers, le serveur FTP, le serveur SMTP, le proxy (filtrage du contenu), ...

La mise en commun a permis de rendre les configurations homogènes.

Conteneurs

Le serveur de mise à jour des bases antivirales (freshclam) s'installe sur le maître.

Le ou les services antivirus s'installent dans les conteneur qui en ont l'usage.

Sur les modules AmonEcole et AmonHorus, le service clamav-daemon est pré-installé dans les groupes de conteneurs :

- `partage (id=52)` ;
- `internet (id=53)` ;
- `reseau (id=51)`.

C'est au paquet du service qui souhaite utiliser le serveur antivirus de gérer son installation, sa configuration et son démarrage dans le conteneur souhaité.

Activation de clamav dans un conteneur

```
<container name='xxx'>
    <package>eole-antivirus-pkg</package>
    <service>clamav-daemon</service>
    <file filelist='clamav' name='/etc/clamav/clamd.conf'/>
</container>
```

1.2. eole-dhcrelay

Le paquet `eole-dhcrelay` permet la mise en place d'un relais DHCP.

Logiciels et services

Le paquet `eole-dhcrelay` s'appuie sur le service dhcp3-relay.

http://www.isc.org

Historique

Ce service est pré-installé sur le module Amon.

Conteneurs

Le service s'installe sur le maître.

1.3. eole-dns

Le paquet `eole-dns` permet la mise en place d'un serveur DNS local.

Logiciels et services

Le paquet `eole-dns` s'appuie principalement sur le service bind9.

http://www.bind9.net/

Historique

À la base, uniquement disponible sur les modules Amon et AmonEcole, ce paquet a été adapté afin d'être installé sur n'importe quel module EOLE, y compris en *mode une carte*.

Conteneurs

Le service est configuré pour s'installer dans le conteneur : `dns (id=18)`.

Sur les modules AmonEcole et AmonHorus, il est installé dans le groupe de conteneurs : `internet (id=53)`.

1.4. eole-exim

Le paquet `eole-exim` permet la mise en place d'un serveur SMTP Exim.

Logiciels et services

Le paquet `eole-exim` s'appuie principalement sur le service exim4.

http://www.exim.org/

Historique

Utilisé à la base sur les modules Scribe et Seshat, le paquet `eole-exim` est désormais utilisé sur tous les modules.

Conteneurs

Le service est configuré pour s'installer dans le conteneur : `mail (id=13)`.

Sur le module AmonEcole et ses variantes, il est installé dans le groupe de conteneurs : `reseau (id=51)`.

1.5. eole-nut

Le paquet `eole-nut` permet la mise en place de la gestion des onduleurs.

La gestion des onduleurs fait l'objet d'une documentation dédiée : GestionDesOnduleurs.

Logiciels et services

Le paquet `eole-nut` s'appuie sur le service upsd.

http://www.networkupstools.org/

Historique

Ce paquet est pré-installé sur tous les modules depuis la version 2.3 d'EOLE.

Conteneurs

Le service s'installe sur le système hôte (maître).

1.6. eole-proxy

Le paquet `eole-proxy` permet la mise en place d'un serveur proxy complet.

La gestion du proxy et du filtrage web fait l'objet d'une documentation dédiée : Proxy.

Logiciels et services

Le paquet `eole-proxy` s'appuie sur les services suivants :

- Squid : proxy cache ;
- e2guardian : filtrage web ;
- Lightsquid : analyseur de logs ;
- smbd, nmbd, winbind, krb5 : authentification NTLM/KERBEROS.

http://www.squid-cache.org/

http://e2guardian.org

http://lightsquid.sourceforge.net/

Historique

A la base, uniquement disponible sur les modules Amon et AmonEcole, ce paquet a été adapté pour être installé sur n'importe quel module EOLE, y compris en **mode une carte**.

Conteneurs

Le service est configuré pour s'installer dans le conteneur : `proxy (id=20)`.

Sur les modules AmonEcole et AmonHorus, il est installé dans le groupe de conteneurs : `internet (id=53)`.

En mode conteneur, l'accès à ces services nécessite la configuration d'une adresse spécifique sur le réseau cible (variable : `adresse ip proxy link`).

Remarques

Afin d'assurer l'authentification en mode NTLM/KERBEROS, ce paquet fournit des configurations Samba

incompatibles avec celles d'`eole-fichier`.

Si l'on souhaite installer `eole-proxy` et `eole-fichier` sur un même serveur, il est impératif qu'ils soient déclarés dans des conteneurs différents. Leur cohabitation est impossible en *mode non conteneur*.

1.7. eole-radius

Le paquet `eole-radius` permet la mise en place d'un serveur RADIUS[p.312].

Logiciels et services

Le paquet `eole-radius` s'appuie sur le projet FreeRADIUS.

http://freeradius.org/

Historique

Ce paquet est pré-installé sur le module Amon.

Conteneurs

Le service s'installe sur le serveur maître.

1.8. eole-reverseproxy

Le paquet `eole-reverseproxy` permet la mise en place d'un serveur proxy inverse.

Le logiciel utilisé, Nginx[p.308], peut aussi faire office de serveur web.

http://nginx.org/

Logiciels et services

Le paquet `eole-reverseproxy` s'appuie sur le serveur Nginx.

Historique

Ce paquet est pré-installé sur les modules Amon, AmonEcole et ses dérivés.

Conteneurs

Le service s'installe sur le système hôte (maître).

1.9. eole-vpn

Le paquet `eole-vpn` permet la mise en place d'un VPN[p.312].

Logiciels et services

Le paquet `eole-vpn` s'appuie principalement sur le logiciel strongSwan[p.313].

Historique

Ce paquet est pré-installé sur les modules Amon, AmonEcole et ses dérivés ainsi que sur le module Sphynx.

Conteneurs

Le service s'installe sur le serveur maître.

1.10. eole-wpad

Le paquet `eole-wpad` permet la mise en place du service de découverte automatique du proxy par les navigateurs (WPAD[p.314]).

Le logiciel utilisé, Nginx[p.308], se charge de distribuer les fichiers `wpad.dat` adaptés à chacun des sous-réseaux.

http://nginx.org/

Logiciels et services

Le paquet `eole-wpad` s'appuie sur le serveur Nginx.

Historique

Ce service étaient auparavant inclus dans le paquet `eole-reverseproxy`. Il peut désormais être installé de façon indépendante.

Le paquet `eole-wpad` est pré-installé sur les modules Amon, AmonEcole et ses dérivés.

Conteneurs

Le service s'installe sur le système hôte (maître).

2. Ports utilisés sur le module Amon

Le module Amon propose de nombreux services.

Ce document donne la liste exhaustive des ports utilisés sur un module Amon standard.

Les ports utilisés sont, dans la mesure du possible, les ports standards préconisés pour les applications utilisées.

Il est possible de lister les ports ouverts sur le serveur par la commande :

`netstat -ntulp`

En mode conteneur, la commande `netstat` listera uniquement les services installés sur le maître.

Ports communs à tous les modules

- 22/tcp : ssh (sshd)
- 25/tcp : smtp (Exim4)
- 68/udp : dhclient
- 123/udp : ntpd
- 3493/tcp : nut (gestion des onduleurs)
- 4200/tcp : ead-web
- 4201/tcp : ead-server
- 4202/tcp : ead-server (transfert de fichiers)
- 5000/tcp : eoleflask/eolegenconfig (application admin)
- 7000/tcp : gen_config
- 8000/tcp : creoled
- 8090/tcp : z_stats (consultation des statistiques Zéphir locales), mise à jour automatique du client Zéphir
- 8443/tcp : EoleSSO

Ports spécifiques au module Amon

- 50/esp : IPsec
- 53/tcp+udp : bind (DNS)
- 67/udp : dhcrelay
- 500/udp : charon (VPN)
- 953/tcp : bind (RNDC)
- 1812/udp : radius
- 1813/tcp+udp : radius accounting
- 3127/tcp : Cntlm (proxy NTLM)
- 3128/tcp : e2guardian (filtrage web)
- 3129/tcp : e2guardian (filtrage web)
- 3401/udp : squid (agent SNMP)
- 4500/udp : charon (VPN)
- 8062/tcp : cgi lightsquid (consultation des statistiques de navigation)
- 8080/tcp : squid (proxy)
- 8081/tcp : squid (proxy)

Le proxy inverse Nginx est susceptible d'écouter sur de nombreux ports afin d'assurer ses missions de redirection :

- 80/tcp : nginx (redirection http)
- 81/tcp : nginx (erreur proxy http)
- 82/tcp : nginx (erreur proxy https)
- 443/tcp : nginx (redirection https)
- 4203/tcp : nginx (redirection vers un EAD)
- 7070/tcp : nginx (redirection vers un portail Envole)
- 8443/tcp : nginx (redirection vers un serveur EoleSSO)

Services et numéro de ports

La correspondance entre un service et un numéro de port standard peut être trouvée dans le fichier `/etc/services`.

Chapitre 9

Questions fréquentes

Certaines interrogations reviennent souvent et ont déjà trouvées une réponse ou des réponses.

1. Questions fréquentes communes aux modules

CAS Authentication failed !

Le message ***`CAS Authentication failed ! You were not authenticated.`*** *(ou* ***`Authentification CAS infructueuse ! Vous n'avez pas été authentifié(e).`*** *)* peut apparaître si des modifications ont été faites dans l'interface de configuration.

Les paramètres constituant un certificat ont été modifiés récemment dans l'interface de configuration du module

La modification, dans l'interface de configuration du module, de l'un des paramètres constituant un certificat (nom de établissement, numéro RNE, etc...) suivie d'une reconfiguration du module ne régénère pas les certificats. Un message explicite le signale lors de l'étape de reconfiguration.

Après changement des paramètres il est nécessaire de supprimer le certificat :

```
# rm -f /etc/ssl/certs/eole.crt
```

puis lancer la reconfiguration du module :

```
# reconfigure
```

Plutôt qu'une suppression, il est possible d'utiliser la commande `gen_certif.py` avec l'option `-f` pour forcer la régénération (cependant, il faut que cette commande soit précédée d'une reconfiguration du module pour que les templates de configuration des certificats soient à jour).

`# reconfigure`

`# /usr/share/creole/gen certif.py -f` ou `# /usr/share/creole/gen certif.py -f nom du certificat` pour la régénération d'un certificat en particulier.

`# reconfigure`

Vous avez ajouté un nom DNS alternatif ou une adresse IP alternative sur le serveur

Il faut ajouter le nom alternatif ou l'adresse IP alternative dans le certificats pour que le certificat le prenne en compte. Pour cela dans l'onglet `Certifs-ssl` en mode expert il faut remplir les champs `Nom DNS alternatif du serveur` et/ou l'adresse `IP alternative du serveur`.

Le bouton `+` permet d'ajouter autant d'alternatives que vous voulez. Il faut ensuite `Valider le groupe` et enregistrer la configuration.

L'opération doit être suivie de la reconfiguration du module, cela va régénérer le certificat `/etc/ssl/certs/eole.crt`

La modification, dans l'interface de configuration du module, de l'un des paramètres constituant un certificat (nom de établissement, numéro RNE, etc...) suivie d'une reconfiguration du module ne régénère pas les certificats. Un message explicite le signale lors de l'étape de reconfiguration.

Après changement des paramètres il est nécessaire de supprimer le certificat :

`# rm -f /etc/ssl/certs/eole.crt`

puis lancer la reconfiguration du module :

`# reconfigure`

Plutôt qu'une suppression, il est possible d'utiliser la commande `gen certif.py` avec l'option `-f` pour forcer la régénération (cependant, il faut que cette commande soit précédée d'une reconfiguration du module pour que les templates de configuration des certificats soient à jour).

`# reconfigure`

`# /usr/share/creole/gen certif.py -f` ou `# /usr/share/creole/gen certif.py -f nom du certificat` pour la régénération d'un certificat en particulier.

`# reconfigure`

Attention, les adresses suivantes ne sont pas définies comme sujet du certificat...

Les paramètres constituant un certificat ont été modifiés récemment dans l'interface de configuration du module

La modification, dans l'interface de configuration du module, de l'un des paramètres constituant un certificat (nom de établissement, numéro RNE, etc...) suivie d'une reconfiguration du module ne régénère pas les certificats. Un message explicite le signale lors de l'étape de reconfiguration.

Après changement des paramètres il est nécessaire de supprimer le certificat :

`# rm -f /etc/ssl/certs/eole.crt`

puis lancer la reconfiguration du module :

`# reconfigure`

Plutôt qu'une suppression, il est possible d'utiliser la commande `gen_certif.py` avec l'option `-f` pour forcer la régénération (cependant, il faut que cette commande soit précédée d'une reconfiguration du module pour que les templates de configuration des certificats soient à jour).

`# reconfigure`

`# /usr/share/creole/gen_certif.py -f` ou `# /usr/share/creole/gen_certif.py -f nom du certificat` pour la régénération d'un certificat en particulier.

`# reconfigure`

Consulter la documentation dédiée aux certificats. (cf. Gestion des certificats SSL)

Une erreur se produit lors de l'instanciation ou d'un reconfigure : "starting firewall : [...] Erreur à la génération des règles eole-firewall !! non appliquées !"

Le message suivant apparaît à l'instance ou au reconfigure après changement de valeurs dans l'interface de configuration du module :

`* starting firewall : bastion (modèle XXX) Erreur à la génération des règles eole-firewall !!`

`non appliquées !`

Vérifier la configuration des autorisations d'accès à SSH et à l'EAD sur les interfaces réseau

Cette erreur provient certainement du masque des variables d'autorisation d'accès à SSH sur l'une des interfaces réseau.

Pour autoriser une seule IP, par exemple `192.168.1.10`, le masque doit être `255.255.255.255` pour autoriser une IP particulière et non 255.255.255.0

Vérifier l'ensemble des autorisations pour l'accès SSH et pour l'accès à l'EAD.

Pour appliquer les changements il faut reconfigurer le module :

`# reconfigure`

La connexion SSH renvoie Permission denied (publickey)

Si les connexions par mots de passe sont interdites, une tentative de connexion sans clé valide entraînera l'affichage du message suivant : `Permission denied (publickey).`

Gestion des mises à jour

Pour connaître la date et l'heure des mises à jour du système il est possible de passer par l'EAD ou par

un terminal.

Via l'EAD

Pour l'afficher il faut se rendre dans la section `Système` / `Mise à jour` de l'EAD.

Dans un terminal

```
python -c "from creole import maj; print maj.get_maj_day()"
```

Pour activer/désactiver la mise à jour hebdomadaire il est possible de passer par l'EAD ou par un terminal.

Via l'EAD

Pour l'afficher il faut se rendre dans la section `Système` / `Mise à jour` de l'EAD.

Dans un terminal

Activation de la mise à jour hebdomadaire :

```
/usr/share/eole/schedule/manage_schedule post majauto weekly add
```

ou :

```
python -c "from creole import maj; maj.enable_maj_auto(); print maj.maj_enabled()"
```

Désactivation de la mise à jour hebdomadaire :

```
/usr/share/eole/schedule/manage_schedule post majauto weekly del
```

ou :

```
python -c "from creole import maj; maj.disable_maj_auto(); print maj.maj_enabled()"
```

Le mot de passe par défaut ne fonctionne pas

Suite à une nouvelle installation le mot de passe par défaut ne fonctionne pas.

Le mot de passe à saisir comprend les dollars devant et derrière : `$eole&123456$`

Échec de la connexion sécurisée

Le navigateur affiche :

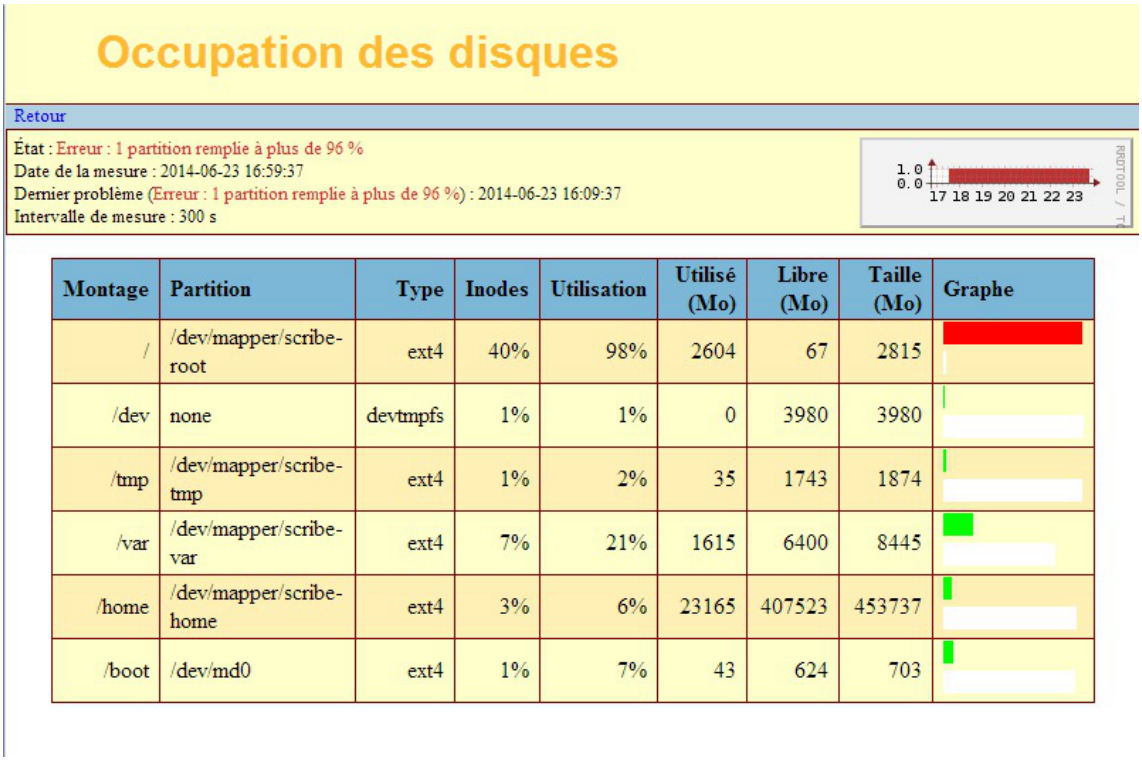
```
Échec de la connexion sécurisée

Une erreur est survenue pendant une connexion à IP:Port.

Vous avez reçu un certificat invalide. Veuillez contacter l'administrateur du serveur ou votre correspondant de messagerie et fournissez-lui les informations suivantes :

Votre certificat contient le même numéro de série qu'un autre certificat émis par l'autorité de certification. Veuillez vous procurer un nouveau certificat avec un numéro de série unique.

(Code d'erreur : sec error reused issuer and serial)
```

Les paramètres constituant un certificat ont été modifiés récemment

La modification, dans l'interface de configuration du module, de l'un des paramètres constituant un certificat (nom de établissement, numéro RNE, etc...) suivie d'une régénération des certificats a eu lieu.

Il faut supprimer le certificat du gestionnaire de certificats du navigateur et recharger la page.

Partition saturée



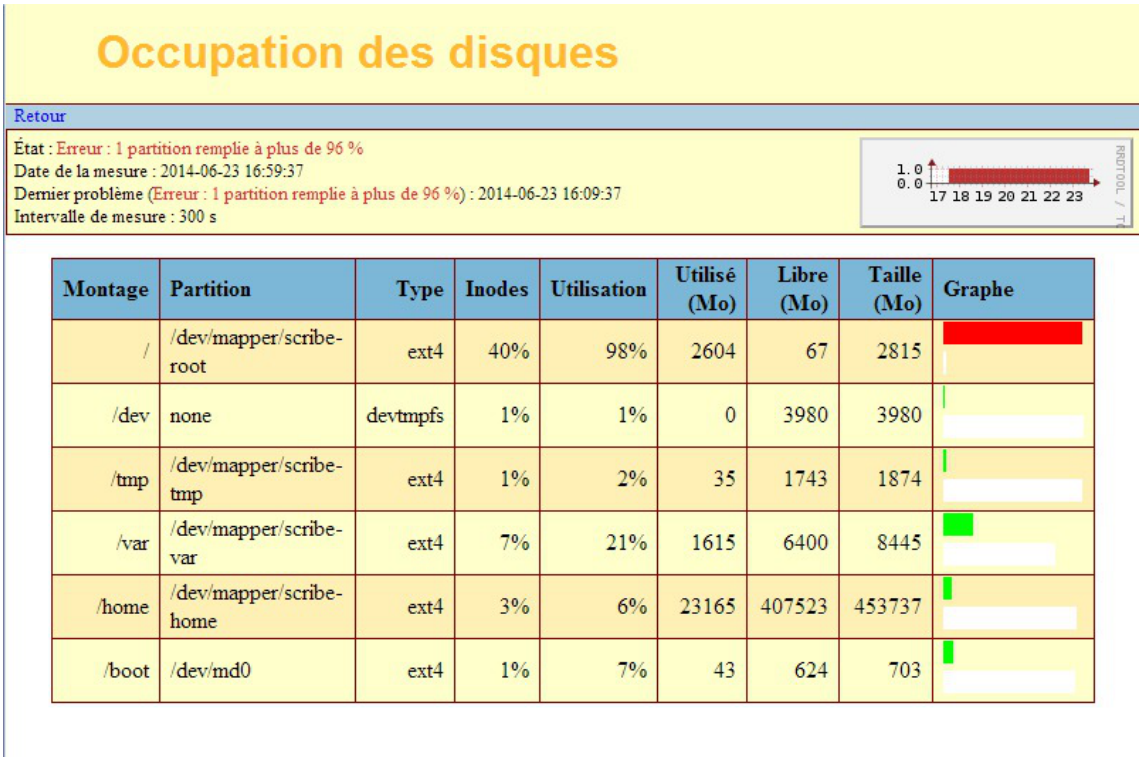
Montage	Partition	Type	Inodes	Utilisation	Utilisé (Mo)	Libre (Mo)	Taille (Mo)	Graphe
/	/dev/mapper/scribe-root	ext4	40%	98%	2604	67	2815	
/dev	none	devtmpfs	1%	1%	0	3980	3980	
/tmp	/dev/mapper/scribe-tmp	ext4	1%	2%	35	1743	1874	
/var	/dev/mapper/scribe-var	ext4	7%	21%	1615	6400	8445	
/home	/dev/mapper/scribe-home	ext4	3%	6%	23165	407523	453737	
/boot	/dev/md0	ext4	1%	7%	43	624	703	

Une partition saturée apparaît en rouge dans l'EAD, la cause peut être :

- le manque de place disponible ;
- le manque d'inodes disponibles.

La cause de la saturation apparaît dans la page Occupation des disques, soit les inodes soit l'utilisation sont à un pourcentage élevé. La résolution du problème est différente selon le cas.

Partition / saturée



Occupation des disques

Retour

État : Erreur : 1 partition remplie à plus de 96 %
Date de la mesure : 2014-06-23 16:59:37
Dernier problème (Erreur : 1 partition remplie à plus de 96 %) : 2014-06-23 16:09:37
Intervalle de mesure : 300 s

Montage	Partition	Type	Inodes	Utilisation	Utilisé (Mo)	Libre (Mo)	Taille (Mo)	Graphe
/	/dev/mapper/scribe-root	ext4	40%	98%	2604	67	2815	
/dev	none	devtmpfs	1%	1%	0	3980	3980	
/tmp	/dev/mapper/scribe-tmp	ext4	1%	2%	35	1743	1874	
/var	/dev/mapper/scribe-var	ext4	7%	21%	1615	6400	8445	
/home	/dev/mapper/scribe-home	ext4	3%	6%	23165	407523	453737	
/boot	/dev/md0	ext4	1%	7%	43	624	703	

Si la partition racine est saturée sans raison apparente et que le taux d'inodes est correct, le montage d'un répertoire avant copie a peut être échoué. La conséquence est que la copie c'est faite sur la partition racine et non sur le montage. Cela peut être le cas, par exemple, de la sauvegarde.

Il faut donc vérifier le contenu et la place occupée par les répertoires (points de montage) `/mnt`, `/mnt/sauvegardes` et `/media` :

Si le répertoire `/mnt/sauvegardes` n'est pas monté il doit être vide :

```
root@scribe:/mnt/sauvegardes# ls -la
total 8 drwxr-xr-x 2 root root 4096 mai 25 11:29 ./ drwxr-xr-x 26 root root 4096 sept. 9 21:07 ../
root@scribe:/mnt/sauvegardes#
```

Normalement le répertoire `/media` ne contient que des sous-dossiers pour le montage des partitions et ou des périphériques.

Pour vérifier l'espace occupé par ces différents répertoires :

```
root@scribe:/# du -h --max-depth=1 /media /mnt/
4,0K /media 4,0K /mnt/
```

Dans certains cas particuliers, la taille allouée à la partition `/` peut être trop juste. Il est possible de revoir la taille des partitions avec l'outil de gestion des volumes logiques (LVM).

Partition /var saturée

Cette partition contient entre autres les journaux systèmes du serveur.

La commande suivante affiche l'espace occupé par chaque répertoire et les classe par taille, le plus grand nombre en dernier (sans tenir compte de l'unité) :

```
# du -smh /var/* | sort -n
```

Un service mal configuré génère une quantité importante de journaux. Si le problème n'est pas résolu la partition va de-nouveau saturer.

Dans certains cas particuliers, la taille allouée à la partition `/var` peut être trop juste. Il est possible de revoir la taille des partitions avec l'outil de gestion des volumes logiques (LVM[p. 307]).

Partition /var saturée en inode

Un nombre important de fichier peut être du à un service mal configuré mais peut aussi être du à un fonctionnement normal. Il faut identifier le répertoire dans lequel il y a le plus de fichier.

La commande suivante affiche le nombre de fichiers par répertoire et les classe par taille, le plus grand nombre en dernier :

```
# for i in $(find /var -type d); do f=$(ls -A $i | wc -l); echo "$f : $i"; done | sort -n
```

Selon les circonstances il faudra soit supprimer des fichiers soit agrandir la partition.

La suppression de fichier ne doit pas être effectué sans connaissances solides du système d'exploitation.

Liste d'arguments trop longue

La commande `# rm -rf /var/<rep>/*` renvoie `Liste d'arguments trop longue`.

Préférez l'utilisation d'une autre commande :

```
# find /var/<rep>/* -type f -name "*" -print0 | xargs -0 rm
```

Le démarrage reste figé à l'étape de vérification des disques

Le serveur est virtualisé avec une solution basée sur l'émulateur qemu.

Seul l'affichage est figé, la machine démarre en fait normalement et est certainement accessible par SSH. Cela vient du support de la carte graphique. Il faut forcer la carte graphique à utiliser une autre carte graphique que celle par défaut (cirrus).

> Sous Proxmox, indiquez carte `VGA standard` à la place de `par défaut`.

Accéder à l'interface de configuration du module depuis un navigateur web

Je n'arrive pas à accéder à l'interface de configuration du module depuis mon navigateur web.

> Pour pouvoir accéder à l'interface de configuration du module depuis un navigateur web il faut que les deux pré-requis suivants soient respectés :
>
> 1. activer l'écoute de l'interface sur l'extérieur en passant la variable `En écoute depuis l'extérieur` à `oui` dans l'onglet `Eoleflask`.
> 2. autoriser votre adresse IP pour administrer le serveur dans l'onglet de l'interface réseau concernée.
>
> Après instance ou reconfigure, l'interface de configuration du module est accessible depuis un navigateur web en HTTPS à l'adresse suivante :
>
> `https://<adresse_serveur>:7000/genconfig/`

Revenir au dernier état fonctionnel du serveur

Un mauvais paramétrage du serveur ne permet plus d'aller au bout de la reconfiguration du module.

> Un fichier `config.eole.bak` est généré dans le répertoire `/etc/eole/` à la fin de l'instanciation et à la fin de la reconfiguration du serveur. Celui permet d'avoir une trace de la dernière configuration fonctionnelle du serveur.
>
> À chaque reconfiguration du serveur un fichier `config.eole.bak.1` est généré, celui-ci est une copie de la configuration fonctionnelle de l'état d'avant.
>
> S'il existe une différence entre `config.eol` et `config.eole.bak` c'est que la configuration du serveur a été modifiée mais qu'elle n'est pas appliquée.

Impossible de trouver la base des matériels maintenue par EOLE

La base des matériels maintenue par EOLE a été supprimée, cette base n'était plus pertinente car elle pouvait contenir du matériel inutilisé comme étant compatible avec les modules EOLE.

Changer le disque dur du serveur

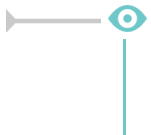
Il est possible entre autre de faire une image avec le logiciel Clonezilla.

> L'UUID[p.314] ayant naturellement changé il faut démarrer en utilisant un LiveCD et éditer l'UUID dans `/etc/fstab` du serveur.

Sources supplémentaires pour apt

Il est possible d'ajouter des sources supplémentaires pour le logiciel apt.

Pour que la solution soit pérenne il faut ajouter dans le répertoire `/etc/apt/sources.list.d/` la description de la nouvelle source dans un fichier portant l'extension `.list`



Par exemple pour avoir à disposition `SCENARIserveur` sur un module EOLE il faut ajouter le fichier `scenari.list` dans le répertoire `/etc/apt/sources.list.d/` avec le contenu suivante :

```
#scenari ppa
deb http://scenari-platform.org/deb precise main
```

Il faut ensuite mettre la liste des paquets disponibles à jour avec la commande `apt-get update`.

Dysfonctionnement des agents suite à un changement d'architecture

En allant sur la page des statistiques de surveillance d'un serveur (EAD ou Application Zéphir), j'obtiens un message du type `rrdtool.error: This RRD was created on another architecture`

Ce problème peut survenir en cas de réinstallation des données d'un serveur 32 bits sur un serveur 64 bits (ou inversement).

Une solution consiste à supprimer les fichiers de statistiques :

- Statistiques propres au serveur Zéphir

  Concerne les statistiques de Zéphir lui-même, pour les statistiques des serveurs clients, l'erreur doit être corrigée sur le client (voir cas suivant).

  ```
  # service zephir stop
  # rm -rf /var/lib/zephir/data/0/*
  # service zephir start
  ```

- Sur un module EOLE autre que Zéphir

  ```
  # service z_stats stop
  # rm -rf /usr/share/zephir/monitor/data/*
  # rm -rf /usr/share/zephir/monitor/stats/*
  # service z_stats start
  ```


Si perdre les statistiques pose problème, il est possible de convertir les fichiers `.rrd` avec l'outil rrdtool.

Depuis l'ancien serveur, pour convertir les fichiers RRD vers des fichiers XML avec la commande `dump` :

```
# rrdtool dump stats.rrd > stats.xml
```

Après les avoir transférés sur le nouveau serveur il faut les convertir en RRD avec la commande `restore` :

```
# rrdtool restore -f stats.xml stats.rrd
```

Le serveur peut maintenant lire le fichier. Vous pouvez le tester avec la commande `info` :

```
# rrdtool info stats.rrd
```

Attention, il y a un (ou plusieurs) fichier par agent.

Exemple sur un serveur Zéphir :

```
root@zephir:~# ls -l /var/lib/zephir/data/0/*/*.rrd -rw-r--r-- 1 root root 11464 août 31 14:51 /var/lib/zephir/data/0/bastion/status.rrd -rw-r--r-- 1 root root 17032 août 31 15:27 /var/lib/zephir/data/0/bilan/status.rrd -rw-r--r-- 1 root root 13576 août 31 15:26 /var/lib/zephir/data/0/debsums/status.rrd -rw-r--r-- 1 root root 1000 août 31 14:51 /var/lib/zephir/data/0/diag/status.rrd -rw-r--r-- 1 root root 13576 août 31 15:26 /var/lib/zephir/data/0/diskspace/status.rrd
[…]
```

Si vous voulez convertir un répertoire entier en XML, utilisez ce petit script bash :

```
# for f in *.rrd; do rrdtool dump ${f} > ${f}.xml; done
```

Source : http://blog.remibergsma.com/2012/04/30/rrdtool-moving-data-between-32bit-and-64bit-archite

Comment débloquer les message en file d'attente ?

Un nombre de messages apparaissent comme étant *Frozen* dans le retour de la commande `diagnose`.

```
*** Messagerie
. Courrier SMTP => Ok
. File d'attente => 1 message(s)
. Messages "Frozen" => 1 message(s)
```

Une solution consiste à récupérer les identifiants des messages :

```
root@scribe:~# exim4 -bp
10h 2.5K 1abJaX-00036S-Bu <> *** frozen ***
touser@ac-test.fr
```

Il est ensuite possible de récupérer les journaux spécifiques message par message :

```
root@scribe:~# exim4 -Mvl 1abJaX-00036S-Bu
2016-03-03 04:06:05 Received from <> R=1abJaX-00036L-8j U=Debian-exim P=local S=2525
2016-03-03 04:06:05 SMTP error from remote mail server after RCPT TO:<touser@ac-test.fr>: host socrate.in.ac-dijon.fr [192.168.57.212]: 554 5.7.1 <touser@ac-test.fr>: Recipient address rejected: Access denied
2016-03-03 04:06:05 touser@ac-test.fr R=satellite_route T=remote_smtp: SMTP error from remote mail server after RCPT
```

```
TO:<touser@ac-test.fr>: host socrate.in.ac-dijon.fr [192.168.57.212]: 554 5.7.1 <touser@ac-test.fr>: Recipient address rejected: Access denied
*** Frozen (delivery error message)
```

Dans cet exemple, le message d'erreur est `Recipient address rejected: Access denied`, l'expéditeur n'est pas autorisé à transiter par la passerelle configurée dans l'interface de configuration du module.

Comment changer le jour de mise à jour d'un serveur EOLE ?

Le jour tiré au hasard pour les mises à jour ne me convient pas et je souhaiterais le changer.

```
root@eole:~# manage_schedule -l
Tâches planifiées EOLE :
 * les tâches hebdomadaires se feront le vendredi à 05:35 (hors sauvegarde)
  - après sauvegarde
   + Mise à jour du serveur (majauto)
root@eole:~#
```

Une solution consiste à supprimer le fichier de configuration `/etc/eole/extra/schedule/config.eol`.

```
root@eole:~# rm /etc/eole/extra/schedule/config.eol
rm : supprimer fichier '/etc/eole/extra/schedule/config.eol' ? y
root@eole:~# manage_schedule -l
Tâches planifiées EOLE :
 * les tâches hebdomadaires se feront le jeudi à 04:12 (hors sauvegarde)
  - après sauvegarde
   + Mise à jour du serveur (majauto)
root@eole:~#
```

2. Questions fréquentes propres au module Amon

Vider le cache du proxy

Vider le répertoire cache de Squid

Il faut arrêter le service Squid, supprimer les fichier et redémarrer le service.

```
# service squid stop
# rm --rf /var/spool/squid/*
# service squid start
```

Problèmes avec le protocole HTTPS

La règle de pare-feu par défaut redirige le trafic Internet directement vers le proxy local.

C'est le mécanisme de proxy transparent.

Cette méthode ne permet toutefois pas de laisser passer le flux chiffré (HTTPS) par ce même mécanisme.

Pour accéder aux sites en HTTPS, il est nécessaire de configurer le proxy sur les postes clients (par exemple : avec ESU sur le module Scribe).

L'option `Destinations non redirigées sur le proxy` disponible en mode expert dans l'onglet `Interface-1` permet, à l'inverse, de déclarer des exceptions.

Lenteur lors de la navigation web

Un filtrage web e2guardian est en place et la navigation web est très lente.

Dans les logs apparaissent des erreurs Squid à répétition (`TCP_DENIED/407`) :

```
Mar  01  10:36:01  amon  (squid):  1363253761.503  51  192.168.10.10 TCP_DENIED/407 4006 GET http://linuxfr.org/ - NONE/- text/html
```

Augmenter le nombre de processus e2guardian maximum dans le filtre

Avant d'augmenter le nombre de processus, on peut vérifier la valeur configurée dans l'interface de configuration du module. Celle-ci est fixée à `256` par défaut et se trouve dans l'onglet `Filtrage web` en mode expert.

Une commande rudimentaire permet de se rendre compte du nombre de processus effectivement exécutés sur le serveur mais elle ne permet pas de distinguer à quelle instance appartiennent les processus et renvoie aussi les processus qui servent a contrôler les autres processus :

```
# ps ax | grep -c guardian
```

La commande `diagnose` permet de connaître précisément le nombre de processus e2guardian exécutés par instance :

```
*** Filtre web
admin: test-eole.ac-dijon.fr => Ok
pedago: test-eole.ac-dijon.fr => Ok
dmz-priv: test-eole.ac-dijon.fr => Ok
. Nb instances 1 => 15/256
```

Si la commande renvoie un nombre trop proche voir supérieur à la valeur configurée dans l'interface de configuration du module, elle doit être augmentée. La valeur maximum est `8192`.

Il est fortement recommandé de ne pas dépasser la valeur maximum de 8192 processus.

Glossaire

AGRIATES *= Accès Généralisé aux Réseaux Internet Académiques et Territoriaux pour les Établissements Scolaires*	De responsabilité partagée entre les collectivités locales et les académies, ces réseaux de concentration des établissements scolaires couvrent à ce jour l'ensemble de lycées et collèges et devraient s'étendre aux secteurs du primaire. L'interconnexion des réseaux AGRIATES de chaque académie forme une partie du réseau RACINE. Par extension, les applications AGRIATES sont les applications Intranet accessibles aux établissements connectés au réseau AGRIATES, à savoir essentiellement, mais pas uniquement, les applications internet à usage des services administratifs des établissements. RACINE-AGRIATES a pour objectif la fourniture d'un support sécurisé pour les échanges d'information (VPN) entre le réseau de l'administration des établissement et leur rectorat de rattachement. L'organisation utilisée pour RACINE-AGRIATES est celle mise en place pour le réseau RACINE. http://www.igc.education.fr/agriates/agriates.htm C'est à la fois une zone de confiance sur le réseau des rectorats et un ensemble de contraintes techniques auxquelles doivent répondre les dispositifs d'accès des établissements. RACINE-AGRIATES fait partie du projet réseau RACINE, dont l'objectif consiste à fournir un support sécurisé pour les échanges d'information (ou Réseau Virtuel Privé (RVP)) entre entités du ministère en s'appuyant sur des infrastructures réseau ouvertes. RACINE-AGRIATES a ainsi pour objectif la fourniture d'un support sécurisé pour les échanges d'information (RVP) entre le réseau de l'administration des établissements et leur rectorat de rattachement. RACINE-AGRIATES rassemble dans une même "zone de confiance" académique les établissements scolaires et les services académiques. Ce nouveau réseau privé virtuel sécurisé est l'Intranet académique.
Anti-spoofing *= Anti-usurpation d'adresse IP*	L'usurpation d'adresse IP est une technique utilisée en informatique qui consiste à envoyer des paquets IP en utilisant une adresse IP source qui n'a pas été attribuée à l'ordinateur qui les émet. Le but peut être de masquer sa propre identité lors d'une attaque d'un serveur, ou d'usurper en quelque sorte l'identité d'un autre équipement du réseau pour bénéficier des services auxquels il a accès. L'anti-spoofing sont des réglages du noyau et du réseau qui permettent de lutter contre l'usurpation d'adresse IP.
ARV *= Administration de Réseaux Virtuels*	ARV permet de construire un modèle de configuration RVP. C'est un logiciel qui permet de générer des configurations RVP pour strongSwan.

	http://www.strongswan.org/
Backbone.js	Backbone est une bibliothèque JavaScript avec une interface RESTful JSON et est basée sur le modèle-vue-contrôleur (MVC). Cette bibliothèque est connu pour être légère, comme sa seule dépendance avec la bibliothèque JavaScript Underscore.js. Elle est conçu pour développer des applications web d'une seule page et permet de maintenir les différentes parties d'applications Web (par exemple, les clients multiples et le serveur) synchronisée. Backbone a été créé par Jeremy Ashkenas, qui est également connu pour CoffeeScript. http://backbonejs.org/
Balise méta	Information sur la nature et le contenu d'une page web, ajoutée dans l'en-tête de la page HTML.
bastion	bastion est un service qui récupère les règles par défaut des zones réseaux utilisées par le module ainsi que toutes les règles personnalisées : • les règles optionnelles de l'EAD ; • les postes et les groupes de postes interdits ou restreints dans l'EAD ; • les règles sur les horaires de l'EAD ; • les règles ipsets (les exceptions sur une directive) ; • les règles de la QOS ; • le règles tcpwrapper (host allow et hosts deny). Le service bastion gère également les règles iptables dans les conteneurs lorsque le module en est pourvu. La liste des actions du service se trouve dans le script `/usr/share/era/bastion.sh`. Le service bastion met en cache les règles mais ne les régénère pas à chaque fois. Seules les commandes `CreoleService bastion restart` ou `service bastion restart` vont régénérer les règles.
broadcast	le broadcast désigne une méthode de transmission de données à l'ensemble des machines d'un réseau. Les protocoles de communications réseau prévoient une méthode simple pour diffuser des données à plusieurs machines en même temps (multicast). Au contraire d'une communication « Point à Point » (unicast), il est possible d'adresser des paquets de données à un ensemble de machines d'un même réseau uniquement par des adresses spécifiques qui seront interceptées par toutes les machines du réseau ou sous-réseau. Source : http://fr.wikipedia.org/wiki/Broadcast_(informatique)
CIDR	La notation CIDR permet de diminuer la taille de la table de routage

= Classless Inter-Domain Routing	contenue dans les routeurs. Elle donne le numéro du réseau suivi par une barre oblique (/) et le nombre de bits à 1 dans la notation binaire du masque de sous-réseau. Le masque 255.255.224.0, équivalent en binaire à 11111111.11111111.11100000.00000000, sera donc représenté par /19 (19 bits à la valeur 1, suivis de 13 bits 0). Source : http://fr.wikipedia.org/wiki/Sous-réseau
Cntlm	Cntlm proxy d'authentification NTLM rapide écrit en C. Il s'intercale entre le poste client et le proxy. Il oblige l'utilisateur à renseigner son identifiant/mot de passe dans une fenêtre surgissante (popup). Il ouvre une socket en écoute et gère la transmission de chaque requête au proxy parent. Si une connexion au proxy parent est créée à nouveau et authentifiée, la connexion précédente est mise en cache et est réutilisée pour une plus grande efficacité. Cntlm intègre également la redirection transparente de port TCP/IP. Il existe de nombreuses fonctions avancées telles que le support de NTLMv2, la protection de mot de passe, le hachage de mot de passe,etc. Il est peu gourmand en terme de ressources. http://cntlm.sourceforge.net/
Conteneur *= LXC*	Un conteneur est une zone isolée à l'intérieur du système qui a un espace spécifique du système de fichier, un réseau, des processus, des allocations mémoires et processeurs, comme s'il s'agissait de plusieurs serveurs physiques séparés. Contrairement à la virtualisation, une seule instance du noyau est présente pour l'ensemble des conteneurs et du maître.
CPU *= Central Processing Unit*	Le CPU , ou en français UCT pour Unité Centrale de Traitement, désigne le ou les microprocesseurs d'un ordinateur. C'est lui qui exécute les programmes informatiques.
Creole *= Création EOLE*	Creole gère la personnalisation des options de configuration des modules, le redémarrage des services, l'installation de paquets additionnels, la mise à jour du système. Il a été conçu pour être facilement personnalisable pour l'utilisateur final. Un ensemble d'outils est proposé pour modifier ou étendre les fonctionnalités offerte par EOLE.
CRL	Acronyme : Certificate Revocation List Une CRL ou Liste de Certificats Révoqués (LCR) est une liste, datée et signée par une Autorité de Certification, des numéros de série des certificats révoqués (mis en opposition) et non expirés, mise à jour périodiquement.
DHCP	Dynamic Host Configuration Protocol (DHCP) est un protocole réseau dont le rôle est d'assurer la configuration automatique des paramètres

= Dynamic Host Configuration Protocol	IP d'une station, notamment en lui affectant automatiquement une adresse IP et un masque de sous-réseau. DHCP peut aussi configurer l'adresse de la passerelle par défaut et des serveurs de noms DNS.
Directive optionnelle	Directive paramétrée dans ERA et qui peut être activée ou désactivée depuis une autre interface. Les directives optionnelles le sont depuis l'EAD et les directives optionnelles cachés le sont dans template `active_tags` des modules Amon et AmonEcole.
DMZ *= Demilitarized Zone*	En informatique, une zone démilitarisée est un sous-réseau séparé du réseau local et isolé de celui-ci et d'Internet par un pare-feu. Ce sous-réseau contient les machines étant susceptibles d'être accédées depuis Internet. Le pare-feu bloquera donc les accès au réseau local pour garantir sa sécurité. Les services susceptibles d'être accédés depuis Internet seront situés en DMZ. En cas de compromission d'un des services dans la DMZ, le pirate n'aura accès qu'aux machines de la DMZ et non au réseau local. Source Wikipédia : http://fr.wikipedia.org/wiki/Zone démilitarisée (informatique)
DNS *= Domain Name System*	Un DNS est un service permettant de traduire un nom de domaine en informations de plusieurs types. L'usage le plus fréquent étant la traduction d'un nom de domaine en adresses IP. Source : http://fr.wikipedia.org/wiki/Dns
e2guardian	e2guardian est un fork de DansGuardian. La dernière version stable de DansGuardian est sortie depuis un très long moment (2009) et plus récemment, suite au désengagement du créateur originel Daniel Barron, le projet a été migré sur la plateforme sourceforge et repris en main par un nouveau mainteneur. DansGuardian devait devenir un projet plus communautaire mais après diverses versions alpha le projet n'a pas réellement repris vie. Depuis 2012 le travail a repris pour incorporer toutes les évolutions et corrections proposées par de nombreux contributeurs et le logiciel est publié sous le nom de e2guardian. http://e2guardian.org
EAD *= EOLE ADmin*	L'EAD est l'interface d'administration des modules EOLE. Il s'agit d'une interface web, accessible uniquement en HTTPS avec un navigateur web à l'adresse `https://<adresse_module>:4200`. L'authentification peut être locale et/ou au travers d'EoleSSO (authentification unique). L'EAD est composé de deux parties : • un serveur de commandes (service ead-server), présent et actif sur tous les modules ; • une interface web (service ead-web), présent et actif sur tous les modules.

	Chaque module dispose d'une interface utilisateur EAD. Certains modules (Zéphir, Sphynx, ...) ne disposent que de la version de base qui permet d'effectuer les tâches de maintenance (mise à jour du serveur, diagnostic, arrêt du serveur, ...). Une version plus complète existe pour les autres modules (Horus, Scribe, Amon, ...) incluant des fonctionnalités supplémentaires.
ELF *= Executable and Linkable Format*	ELF est un format de fichier binaire utilisé pour l'enregistrement de code compilé
ERA *= Éditeur de Règles pour le module Amon*	ERA est une application graphique de génération et de gestion de règles de sécurité adaptée au module pare-feu Amon. À partir du fichier XML de description du pare-feu, un script de règles iptables pour Netfilter est généré de manière à implémenter ces règles sur le module pare-feu Amon. La génération directe de règles iptables est également possible, permettant d'utiliser ERA pour d'autres types de serveurs sous GNU/Linux.
ESU *= Environnements Sécurisés des Utilisateurs*	Environnement Sécurisé des Utilisateurs (ESU) est un projet initialement développé par Olivier Adams du CRDP de Bretagne qui est maintenant publié par EOLE et distribué sous licence CeCILL. Cet outil permet aux administrateurs de réseaux en établissement scolaire de définir (très simplement) les fonctions laissées disponibles aux utilisateurs des postes informatiques. ESU propose de nombreuses fonctions : • limitation des accès aux paramètres de Windows (panneau de configuration...) ; • définition par salle ou par poste des lecteurs réseaux, icônes du bureau, menu démarrer et limitation des fonctions ; • configuration des imprimantes partagées sur les postes ; • configuration des navigateurs (Internet Explorer et Mozilla Firefox) ; • éditeur de règles permettant de rajouter autant de règles que vous le souhaitez.
Extrémité	Une extrémité est un sous ensemble d'une zone. Elle est définie par une ou plusieurs adresses IP ou bien un sous-réseau. Elle hérite du niveau de sécurité de la zone à laquelle elle appartient.
Filtrage syntaxique	Système de pondération détectant des mots interdits dans une page et lui assignant un score en fonction de la gravité et du nombre de mots détectés. Le proxy bloquera les pages dont le score dépasse un certain seuil.
Flask	Flask est un framework d'application web léger écrit en Python et basé sur le toolkit Werkzeug (une librairie Python WSGI) et sur le moteur de template Jinja2.

	Flask est appelé microframework parce qu'il garde un cœur simple, mais extensible. Il n'y a aucune couche d'abstraction de données, pas de formulaire de validation ou tout autre composant que des bibliothèques tierces ne traitent déjà. Cependant, Flask supporte les extensions, ce qui permet d'ajouter des fonctionnalités si elles sont mises en œuvre dans Flask lui-même. Il existe des extensions pour utiliser les objets relationnels, valider des formulaires, le téléchargement, diverses technologies d'authentification ouvertes, et plus encore. Flask est sous licence BSD. http://flask.pocoo.org/
Flux	Lien entre deux zones.
Flux descendant	Interactions d'un niveau de sécurité plus fort vers un niveau de sécurité plus faible avec une politique par défaut "autorisé".
Flux montant	Interactions d'un niveau de sécurité plus faible vers un niveau de sécurité plus fort avec une politique par défaut "interdit".
HTTP *= HyperText Transfer Protocol - protocole de transfert hypertexte*	HTTP est un protocole de communication client-serveur développé pour le World Wide Web. HTTPS (le S signifiant sécurisé) est la variante du HTTP sécurisée par l'usage des protocoles SSL ou TLS. HTTP est un protocole de la couche application. Dans les faits on utilise le protocole TCP comme couche de transport. Un serveur HTTP utilise alors par défaut le port 80 (443 pour HTTPS).
ICMP *= Internet Control Message Protocol*	Internet Control Message Protocol est l'un des protocoles fondamentaux constituant la suite de protocoles Internet. Il est utilisé pour véhiculer des messages de contrôle et d'erreur pour cette suite de protocoles, par exemple lorsqu'un service ou un hôte est inaccessible.
INI	Un fichier INI est un fichier de configuration dans un format de données introduit par les systèmes d'exploitation Windows en 1985. Par convention les noms de ces fichiers portent l'extension « `.ini` ». Les fichiers INI sont des fichiers texte qui peuvent être manipulés avec un logiciel courant de type éditeur de texte. La valeur de chaque paramètre de configuration est indiquée par une formule : paramètre = valeur. Source Wikipédia : http://fr.wikipedia.org/wiki/Fichier_INI
instance *= instanciation, instancier*	Instancier un serveur correspond à la troisième étape de mise ne œuvre d'un module EOLE. Cette phase permet d'écrire les fichiers de configuration et de lancer ou de redémarrer les services d'après les valeurs renseignées lors de l'étape de configuration. L'instanciation prépare le système en vue de sa mise en production et s'exécute à l'aide de la commande `instance`.

iptables	iptables est un logiciel libre grâce auquel l'administrateur système peut configurer les chaînes et règles dans le pare-feu dans l'espace noyau composé par des modules Netfilter. Netfilter est un framework implémentant un pare-feu au sein du noyau Linux à partir de la version 2.4 de ce dernier. Il prévoit des accroches (hooks) dans le noyau pour l'interception et la manipulation des paquets réseau lors des appels des routines de réception ou d'émission des paquets des interfaces réseau.
IPv6 *= Internet Protocol version 6*	L'IPv6 est un protocole réseau sans connexion de la couche 3 du modèle OSI. IPv6 est le successeur d'IPv4. Grâce à des adresses de 128 bits au lieu de 32 bits, IPv6 dispose d'un espace d'adressage bien plus important qu'IPv4. Cette quantité d'adresses considérable permet une plus grande flexibilité dans l'attribution des adresses et une meilleure agrégation des routes dans la table de routage d'Internet. La traduction d'adresse, qui a été rendue populaire par le manque d'adresses IPv4, n'est plus nécessaire. IPv6 dispose également de mécanismes d'attribution automatique des adresses et facilite la renumérotation. La taille du sous-réseau, variable en IPv4, a été fixée à 64 bits en IPv6. Les mécanismes de sécurité comme IPsec font partie des spécifications de base du protocole. L'en-tête du paquet IPv6 a été simplifié et des types d'adresses locales facilitent l'interconnexion de réseaux privés.
L'expérience à tâtons	Ne pouvant établir avec certitude qui de l'équipe a introduit ce type d'expérience dans la documentation du module Amon en version 2.2, l'équipe dans son intégralité revendique la paternité du concept.
LDAP *= Lightweight Directory Access Protocol*	À l'origine un protocole permettant l'interrogation et la modification des services d'annuaire, LDAP a évolué pour représenter une norme pour les systèmes d'annuaires.
Liste blanche	Une liste blanche est une liste d'adresse web autorisées par le proxy.
Liste noire	Une liste noire est un document rassemblant les noms d'entités concrètes ou virtuelles jugés indésirables. Dans le contexte informatique une liste noire est une liste d'adresses web indésirables qui seront bloquées par le proxy.
LVM *= Logical Volume Management*	La gestion par volumes logiques est à la fois une méthode et un logiciel. Elle permet le découpage, la concaténation, le redimensionnement et l'utilisation des espaces de stockage. Le logiciel permet de gérer, de sécuriser et d'optimiser de manière souple les espaces de stockage sur les systèmes d'exploitation de type UNIX.
Marionette	Marionette simplifie le code applicatif Backbone grâce à des vues robustes et des solutions d'architecture.

	http://marionettejs.com/
Modèle	ERA enregistre la description d'un pare-feu dans un fichier XML situé par défaut dans un répertoire nommé `/usr/share/era/modeles/`. Ce fichier est souvent dérivé d'un modèle livré de base, fichiers de référence présent dans le dossier `/usr/share/era/modeles` sur lequel se base l'utilisateur. Par extension, un modèle est n'importe quel fichier de description de pare-feu dans ERA.
MTU *= Maximum Transmission Unit*	La MTU définit la taille maximum du paquet (en octet) pouvant être transmis sur le réseau sans fragmentation. Pour plus d'information : http://fr.wikipedia.org/wiki/Maximum_Transmission_Unit
NAS *= Network Access Server*	Un Network Access Server (NAS), ici un switch, fonctionne comme un client RADIUS. Au sein d'un réseau, le premier équipement qui prend en charge un client (machine ou utilisateur) est un équipement d'accès (switch, point d'accès Wifi). Ces équipements jouent un rôle crucial car ce sont eux qui détectent la présence d'un équipement qui essaye de rejoindre le réseau. Ils interviennent donc dans le processus d'authentification. Dans la terminologie RADIUS, ces équipements d'accès sont appelés NAS (Network Access Server), ou clients Radius : ce sont ces équipements qui interagissent avec le serveur RADIUS en utilisant le protocole du même nom. Ils devront d'ailleurs être configurés pour cela (ils doivent connaître l'adresse IP du serveur Radius). Source : http://juboite.hd.free.fr/doku.php?id=tuto:radius:freeradius
NAT *= Network Address Translation*	Le NAT est un mécanisme informatique permettant de faire communiquer un réseau local avec l'Internet. En réseau informatique, on dit qu'un routeur fait de la traduction d'adresse réseau lorsqu'il fait correspondre les adresses IP internes non-uniques et souvent non routables d'un intranet à un ensemble d'adresses externes uniques et routables. Ce mécanisme permet notamment de faire correspondre une seule adresse externe publique visible sur Internet à toutes les adresses d'un réseau privé, et pallie ainsi l'épuisement des adresses IPv4. Source Wikipédia : http://fr.wikipedia.org/wiki/Network_address_translation
Netfilter	Netfilter est un outil de filtrage de paquets sous linux. Le logiciel qui lui est associé est iptables.
Nginx *= Engine-x*	Nginx est un logiciel de serveur Web ainsi qu'un proxy inverse. Le serveur est de type asynchrone par opposition aux serveurs synchrones où chaque requête est traitée par un processus dédié. Donc au lieu d'exploiter une architecture parallèle et un multiplexage

	temporel des tâches par le système d'exploitation, Nginx utilise les changements d'état pour gérer plusieurs connexions en même temps. Le traitement de chaque requête est découpé en de nombreuses tâches plus petites ce qui permet de réaliser un multiplexage efficace entre les connexions. Pour tirer parti des ordinateurs multiprocesseurs, le serveur permet de démarrer plusieurs processus. Ce choix d'architecture se traduit par des performances très élevées, une charge et une consommation de mémoire particulièrement faibles comparativement aux serveurs Web classiques, tels qu'Apache.
Niveau de sécurité	Nombre entier (entre 0 et 100) permettant d'ordonner les zones par ordre croissant.
Nom de domaine	Dans le système de noms de domaine, un nom de domaine (NDD en notation abrégée française ou DN pour Domain Name en anglais) est un identifiant de domaine internet. Un domaine est un ensemble d'ordinateurs reliés à Internet et possédant une caractéristique commune. Voici des exemples de domaine : le domaine .fr est l'ensemble des ordinateurs hébergeant des activités pour des personnes ou des organisations qui se sont enregistrées auprès de l'AFNIC qui est le registre responsable du domaine de premier niveau .fr ; en général, ces personnes ou ces entreprises ont une certaine relation (qui peut être ténue dans certains cas) avec la France ; le domaine paris.fr est l'ensemble des ordinateurs hébergeant des activités pour la ville de Paris. Un nom de domaine est un « masque » sur une adresse IP. Le but d'un nom de domaine est de retenir et communiquer facilement l'adresse d'un ensemble de serveurs (site web, courrier électronique, FTP...). Par exemple, wikipedia.org est plus simple à mémoriser que 91.198.174.2. Source Wikipédia : http://fr.wikipedia.org/wiki/Nom_de_domaine
NTLM *= NT Lan Manager*	NTLM est un protocole d'identification utilisé dans diverses implémentations des protocoles réseau Microsoft. Il est aussi utilisé partout dans les systèmes de Microsoft comme un mécanisme d'authentification unique SSO.
NTP *= Network Time Protocol*	NTP est un protocole permettant de synchroniser les horloges des systèmes informatiques.
NUT *= Network UPS Tools*	NUT est un ensemble d'outils permettant de monitorer un système relié à un ou des onduleurs. Il se compose de plusieurs éléments : • le démon `nut` lancé au démarrage du système ; • le démon `upsd` qui permet d'interroger l'onduleur, il est lancé

	sur le PC relié à l'onduleur ; • le démon `upsmon` qui permet de monitorer et lancer les commandes nécessaires sur le réseau ondulé (arrêt de machines ...) ; • différents programmes pour envoyer des commandes manuellement à l'onduleur. `upsd` peut communiquer avec plusieurs onduleurs si nécessaire. `upsmon` interroge à intervalle régulier la machine du réseau sur laquelle est lancée `upsd`.
OSPF *= Open Shortest Path First*	Open Shortest Path First (OSPF) est un protocole de routage interne IP de type « à état de liens ». Dans OSPF, chaque routeur établit des relations d'adjacence avec ses voisins immédiats en envoyant des messages hello à intervalle régulier. Chaque routeur communique ensuite la liste des réseaux auxquels il est connecté par des messages Link-state advertisements (LSA) propagés de proche en proche à tous les routeurs du réseau. L'ensemble des LSA forme une base de données de l'état des liens Link-State Database (LSDB) pour chaque aire, qui est identique pour tous les routeurs participants dans cette aire. Chaque routeur utilise ensuite l'algorithme de Dijkstra, Shortest Path First (SPF) pour déterminer la route la plus courte vers chacun des réseaux connus dans la LSDB. Le bon fonctionnement d'OSPF requiert donc une complète cohérence dans le calcul SPF, il n'est donc par exemple pas possible de filtrer des routes ou de les résumer à l'intérieur d'une aire. En cas de changement de topologie, de nouveaux LSA sont propagés de proche en proche, et l'algorithme SPF est exécuté à nouveau sur chaque routeur. Source Wikipédia : http://fr.wikipedia.org/wiki/Open_Shortest_Path_First
OTP *= One-time password*	Un Mot de passe unique (OTP) est un mot de passe qui n'est valable que pour une session ou une transaction. Les OTP permettent de combler certaines lacunes associées aux traditionnels mots de passe statiques, comme la vulnérabilité aux attaques par rejeu. Cela signifie que, si un intrus potentiel parvient à enregistrer un OTP qui était déjà utilisé pour se connecter à un service ou pour effectuer une opération, il ne sera pas en mesure de l'utiliser car il ne sera plus valide. En revanche, les OTP ne peuvent pas être mémorisé par les êtres humains, par conséquent, ils nécessitent des technologies complémentaires afin de s'en servir. Source : http://fr.wikipedia.org/wiki/Mot_de_passe_unique
Pare-feu *= firewall*	Un pare-feu est un logiciel et/ou un matériel, permettant de faire respecter la politique de sécurité du réseau, celle-ci définissant quels

	sont les types de communication autorisés sur ce réseau informatique. Il a pour principale tâche de contrôler le trafic entre différentes zones de confiance, en filtrant les flux de données qui y transitent. Généralement, les zones de confiance incluent Internet (une zone dont la confiance est nulle) et au moins un réseau interne (une zone dont la confiance est plus importante). Le but est de fournir une connectivité contrôlée et maîtrisée entre des zones de différents niveaux de confiance, grâce à l'application de la politique de sécurité et d'un modèle de connexion basé sur le principe du moindre privilège. Le filtrage se fait selon divers critères. Les plus courants sont : • l'origine ou la destination des paquets (adresse IP, ports TCP ou UDP, interface réseau, etc.) ; • les options contenues dans les données (fragmentation, validité, etc.) ; • les données elles-mêmes (taille, correspondance à un motif, etc.) ; • les utilisateurs pour les plus récents. Source Wikipédia : http://fr.wikipedia.org/wiki/Pare-feu_(informatique)
Politique de filtrage	Une politique de filtrage permet de définir une suite d'autorisation et d'interdiction dans les accès web.
PPPoE *= Point-to-Point Protocol over Ethernet*	PPPoE est un protocole d'encapsulation de PPP sur Ethernet. Il permet de bénéficier des avantages de PPP et du contrôle de la connexion (débit, etc.), sur un réseau 802.3. Il est beaucoup employé par les connexions haut débit à Internet par ADSL et câble destinées aux particuliers, bien qu'une connexion utilisant un pont Ethernet-Ethernet soit souvent plus stable et plus performante. Il pose également des problèmes de MTU.
Préfixe binaire	Les préfixes binaires (kibi-, mébi-, gibi-, tébi-, pébi- et exbi-) sont souvent utilisés lorsqu'on a affaire à de grandes quantités d'octets. Ils sont dérivés, tout en étant différents, des préfixes du système international (kilo-, méga-, giga- et ainsi de suite). La raison d'être de ces préfixes binaires est d'éviter la confusion de valeur avec les préfixes du système international. http://fr.wikipedia.org/wiki/Préfixe_binaire
Pronote	Pronote est un logiciel privateur de gestion de vie scolaire créé en 1999. C'est au départ un client lourd, mais il existe, depuis 2003, une extension permettant d'utiliser une version Web.
Proxy sibling *= proxy frère*	Hiérarchiquement, un cache interrogé peut être un de niveau supérieur (parent) ou de niveau égal (frère ou sibling).

	Les serveurs parents sont d'ordinaire plus proches du serveur hébergeant l'objet recherché que les serveurs fils. Si un serveur fils ne peut trouver l'objet, la requête est en général relayée vers un serveur de cache parent qui va rapporter, mémoriser (mettre en cache) et finalement transmettre la requête au demandeur. Les serveurs frères (siblings) sont des serveurs de cache d'un niveau hiérarchique égal, dont le but est de répartir la charge. http://fr.wikipedia.org/wiki/Internet_Cache_Protocol
PUA *= Potentially Unwanted Applications*	Applications potentiellement indésirables.
Qualité de service *= QOS*	Régulation des flux du trafic sur un réseau, définition de Wikpedia [http://fr.wikipedia.org/wiki/QoS]
RADIUS *= Remote Authentication Dial-In User Service*	RADIUS est un protocole client-serveur permettant de centraliser des données d'authentification. Source : http://fr.wikipedia.org/wiki/Remote_Authentication_Dial-In_User_Servic
Réseau virtuel Privé *= RVP ou VPN (Virtual Private Network) en anglais*	Le réseau virtuel privé permet de relier au travers d'Internet des sous réseaux entre eux, de façon sécurisée et chiffrée.
RIP *= Routing Information Protocol*	RIP, protocole d'information de routage, est un protocole de routage IP de type Vector Distance (à vecteur de distances) s'appuyant sur l'algorithme de détermination des routes décentralisé. Il permet à chaque routeur de communiquer aux routeurs voisins la métrique, c'est-à-dire la distance qui les sépare d'un réseau IP déterminé quant au nombre de sauts ou « hops » en anglais.Pour chaque réseau IP connu, chaque routeur conserve l'adresse du routeur voisin dont la métrique est la plus petite. Ces meilleures routes sont diffusées toutes les 30 secondes. Source Wikipédia : http://fr.wikipedia.org/wiki/Routing_Information_Protocol
Round-robin *= tourniquet*	Round-robin (RR) est un algorithme d'ordonnancement courant dans les systèmes d'exploitation. Ce dernier attribue des tranches de temps à chaque processus en proportion égale, sans accorder de priorité aux processus. Source Wikipédia : http://fr.wikipedia.org/wiki/Round-robin_(informatique)
SAML *= Security assertion markup language*	SAML est un standard informatique définissant un protocole pour échanger des informations liées à la sécurité. Il est basé sur le langage XML. SAML suppose un fournisseur d'identité et répond à la problématique de l'authentification au-delà d'un intranet.
SecurID	SecurID est un système de token, ou authentifieur, produit par la

	société RSA Security et destiné à proposer une authentification forte à son utilisateur dans le cadre de l'accès à un système d'information. Source : http://fr.wikipedia.org/wiki/SecurID
Service	Couple protocole et/ou port (ou plage de ports).
SMTP *= Simple Mail Transfer Protocol*	SMTP est un protocole de communication utilisé pour transférer le courrier électronique vers les serveurs de messagerie électronique.
Squid	Squid est un proxy (serveur mandataire en français) cache sous GNU/Linux. De ce fait il permet de partager un accès Internet entre plusieurs utilisateurs n'ayant qu'une seule connexion. Un serveur proxy propose également un mécanisme de cache des requêtes, qui permet d'accéder aux données en utilisant les ressources locales au lieu des ressources web, réduisant les temps d'accès et la bande passante consommée. Il est également possible aussi d'effectuer des contrôles de sites.
SSH *= Secure Shell*	Secure Shell est à la fois un programme informatique et un protocole de communication sécurisé. Le protocole de connexion impose un échange de clés de chiffrement en début de connexion. Par la suite toutes les trames sont chiffrées. Il devient donc impossible d'utiliser un sniffer pour voir ce que fait l'utilisateur.
StartTLS	Dans certains cas, un même port est utilisé avec et sans SSL. Dans ce cas, la connexion est initiée en mode non chiffré. Le tunnel est ensuite mis en place au moyen du mécanisme StartTLS. C'est le cas, par exemple des protocoles de mails IMAP et SMTP ou LDAP.
strongSwan	strongSwan est une implémentation libre et complète de VPN IPsec pour le système d'exploitation Linux (noyaux Linux 2.6 et 3.x). L'objectif de ce projet est de proposer des mécanismes d'authentification forts. http://www.strongswan.org/
Swap *= Verbe échanger*	En informatique le swap sert à étendre la mémoire utilisable par un système d'exploitation, par un fichier d'échange ou une partition dédiée ; c'est aussi une instruction de certains processeurs et une fonction de certains langages de programmation qui permet l'échange de deux variables.
Tableaux de flux	Ensemble de lien entre les zones permettant de définir une politique par défaut et de classer un ensemble de règles (directives).
Template *= Modèle Creole*	Un template est un fichier contenant des variables Creole, qui sera instancié pour générer un fichier cible (typiquement un fichier de configuration serveur).
Tiramisu	À cause de l'afflux de plus en plus grand des options de configuration des serveurs EOLE (plus de 1600 au dernier recensement), il était

= Outil de gestion de configuration	devenu de plus en plus difficile de correctement récupérer les options et de les utiliser là où elles devaient effectivement être employées. Pour remédier à ces difficultés, l'outil Tiramisu a été développé, il est utilisé comme moteur du générateur de configuration de la version EOLE 2.4. La documentation technique du projet : http://tiramisu.labs.libre-entreprise.org Les sources du projet Tiramisu : http://labs.libre-entreprise.org/projects/tiramisu/
TLS *= Transport Layer Security*	Le TLS et son prédécesseur Secure Sockets Layer (SSL), sont des protocoles de sécurisation des échanges sur Internet. Le TLS est la poursuite des développements de SSL. Par abus de langage, on parle de SSL pour désigner indifféremment SSL ou TLS.
Type MIME	Un type MIME est une information permettant de connaitre le format d'un document sans se baser sur l'extension.
URI *= Uniform Resource Identifier*	L'URI est une courte chaîne de caractères identifiant une ressource sur un réseau.
UUID *= Universally Unique IDentifier*	Le but des UUID est de permettre à des systèmes distribués d'identifier de façon unique une information sans coordination centrale importante. Dans ce contexte, le mot « unique » doit être pris au sens de « unicité très probable » plutôt que « garantie d'unicité ». Source : http://fr.wikipedia.org/wiki/Universal_Unique_Identifier
VLAN *= Réseau local virtuel*	Un VLAN (Virtual Local Area Network) est un réseau local regroupant un ensemble de machines de façon logique et non physique.
WPAD *= Web Proxy Autodiscovery Protocol*	WPAD définit la façon selon laquelle un navigateur web se connecte à Internet. Ce protocole permet au navigateur d'utiliser automatiquement le proxy approprié à l'URL demandée. WPAD laisse le navigateur découvrir l'emplacement du fichier PAC grâce aux services DHCP et DNS. Un fichier PAC est un fichier texte en JavaScript, qui contient entre autres la fonction FindProxyForURL(url, host). Cette fonction possède deux arguments associés : • URL : l'URL de l'objet • HOST : le nom de domaine dérivé de l'URL
XML *= Extensible Markup Language*	L'Extensible Markup Language (« langage de balisage extensible » en français) est un langage informatique de balisage générique qui dérive du SGML. Cette syntaxe est dite « extensible » car elle permet de définir différents espaces de noms, c'est-à-dire des langages avec chacun leur vocabulaire et leur grammaire, comme XHTML, XSLT, RSS, SVG... Elle est reconnaissable par son usage des chevrons (< >) encadrant les balises. L'objectif initial est de faciliter l'échange

	automatisé de contenus complexes (arbres, texte riche...) entre systèmes d'informations hétérogènes (interopérabilité). Avec ses outils et langages associés une application XML respecte généralement certains principes : • la structure d'un document XML est définie et validable par un schéma, • un document XML est entièrement transformable dans un autre document XML. Source : http://fr.wikipedia.org/wiki/Xml
XML-RPC *= XML Remote procedure call*	XML-RPC est un protocole RPC (Remote procedure call), une spécification simple et un ensemble de codes qui permettent à des processus s'exécutant dans des environnements différents de faire des appels de méthodes à travers un réseau. XML-RPC permet d'appeler une fonction sur un serveur distant à partir de n'importe quel système (Windows, Mac OS X, GNU/Linux) et avec n'importe quel langage de programmation. Le serveur est lui même sur n'importe quel système et est programmé dans n'importe quel langage. Cela permet de fournir un Service web utilisable par tout le monde sans restriction de système ou de langage. Source : http://fr.wikipedia.org/wiki/XML-RPC
ZéphirLog	ZéphirLog était un module 2.2 qui permettait de stocker et d'archiver les journaux d'événements remontés par les différents serveurs EOLE.
Zone	Découpage d'un réseau en restant centré sur le pare-feu, le pare-feu lui-même étant une zone nommée par convention **bastion**, c'est la zone la plus sécurisée (niveau 100). Chaque zone est définie par un nom, une adresse réseau, et un niveau de sécurité.