GUIDE D'INSTALLATION DE FIREWALL OPEN SOURCE

Endian firewall

Endian firewall c'est une distribution orientée sécurité, basé sur Ipcop, qui intègre une panoplie d'outils tels que : le Firewall, l'IDS, le Proxy, le VPN, la passerelle antivirale… etc. Dans ce guide on va détailler la mise en place des différents outils de cette distribution afin d'avoir une solution de sécurité complète d'un réseau d'entreprise.

Agence Nationale de la Sécurité Informatique

Gestion de document

Auteur	Version	Date	Modification apportée
K. J	1.0	16/05/2011	Première version

Document Publique

Document Interne

PLAN

Présentation d'Endian

Endian est une distribution de sécurité open source dont le but est d'obtenir une distribution Linux complètement dédiée à la sécurité et aux services essentiels d'un réseau afin d'offrir une protection maximale contre le vol de données, virus, spyware, spam et autres menaces Internet. Plus concrètement, Endian intègre un firewall qui va jouer le rôle d'intermédiaire entre un réseau considéré comme non sûr (Internet) et un réseau que l'on souhaite sécuriser (le réseau local par exemple), tout en fournissant des services permettant la gestion et le suivi de celui-ci qui seront gérer à travers une interface web (Unified Threat Management UTM).

Dans ce guide nous aborderons le fonctionnement des interfaces, l'installation et la configuration d'EFW. Ensuite, nous détaillerons les différents services proposés par Endian.

1. Fonctionnement

La partie firewall d'Endian Firewall se compose de plusieurs interfaces dont chacune peut être ou non utilisée :

- Rouge

  Zone du réseau à risque (Internet).
- Verte

  Zone du réseau à protéger (réseau local).
- Bleu

  Zone spécifique pour les périphériques sans fil (wifi). Il n'est possible de faire communiquer l'interface Verte et l'interface Bleu qu'en créant un VPN.
- Orange

  Zone démilitarisée (DMZ), cette zone isolée, hébergeant des applications mises à disposition du public. Elle est accessible de l'extérieur mais ne possède aucun accès

sortant (serveur web, un serveur de messagerie, un serveur FTP public, etc.).

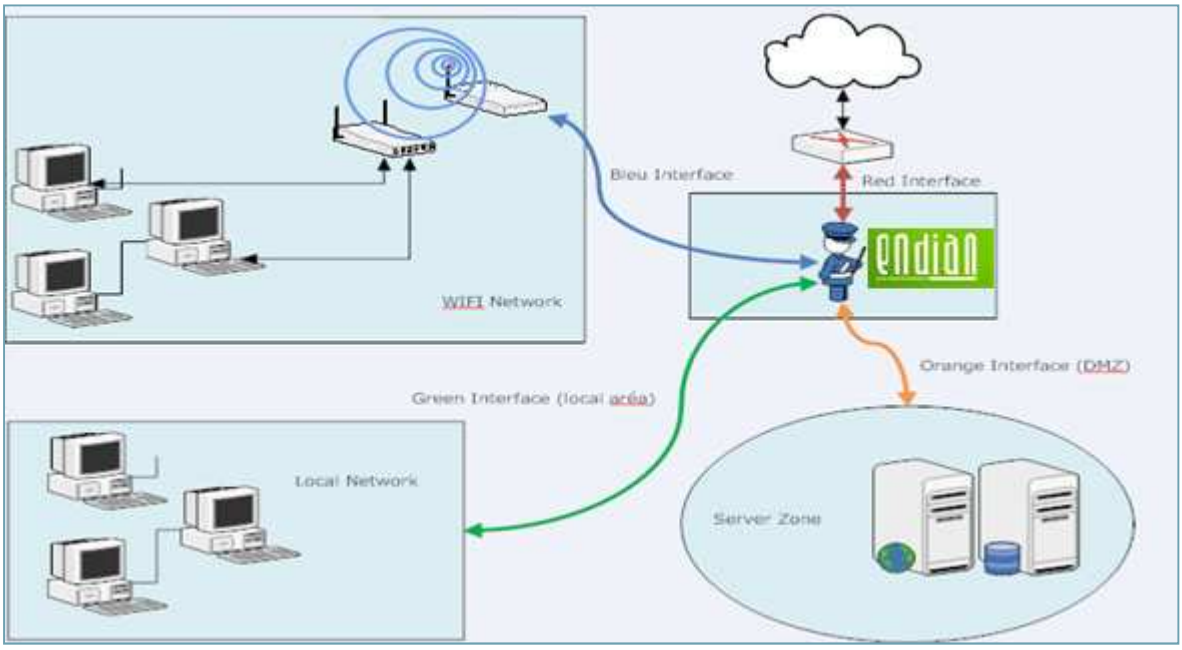
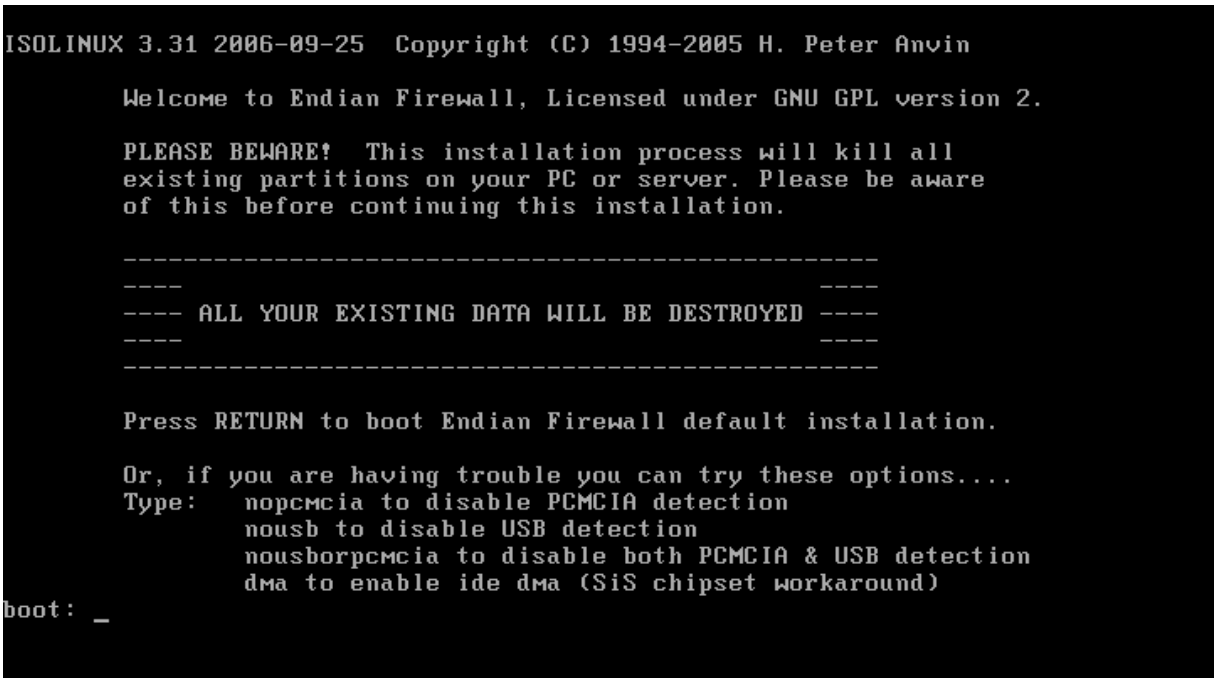


Fig1. Schéma de fonctionnement d'EFW

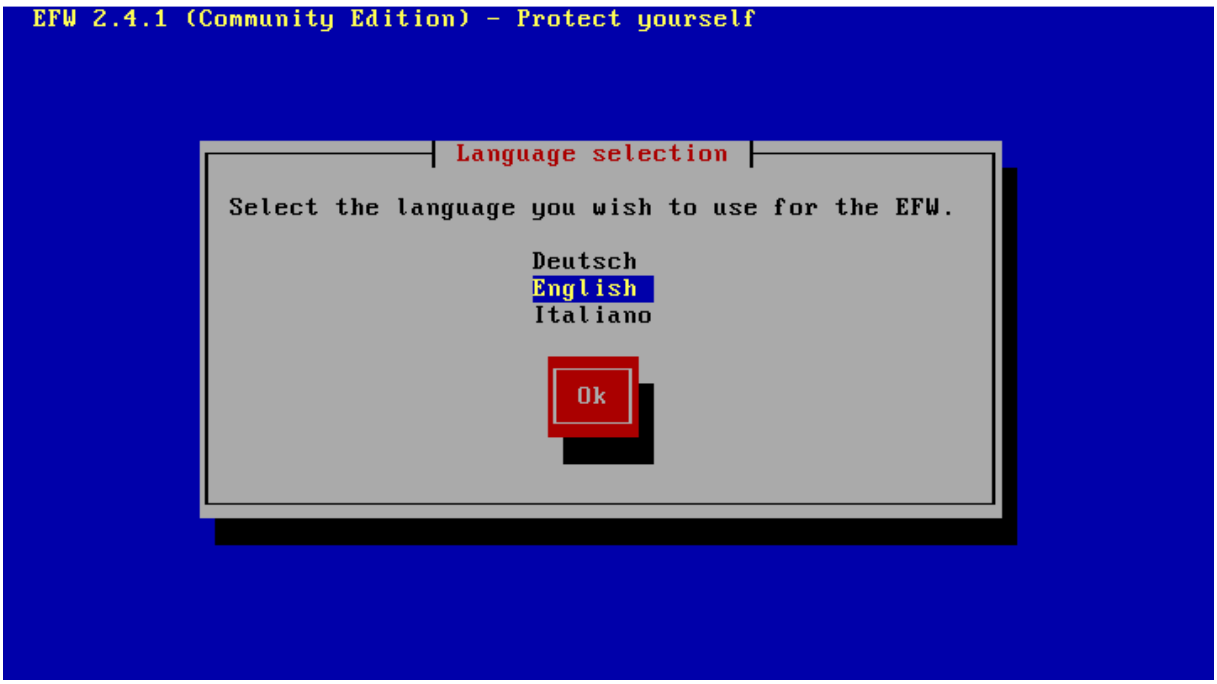
2. Installation

- Téléchargez la dernière version d'Endian firewall depuis son site officiel : http://www.endian.com/en/community/download/
- Une fois le fichier téléchargé, il ne vous reste plus qu'à graver cette image sur un CD.
- Démarrer l'installation sur une machine ayant :

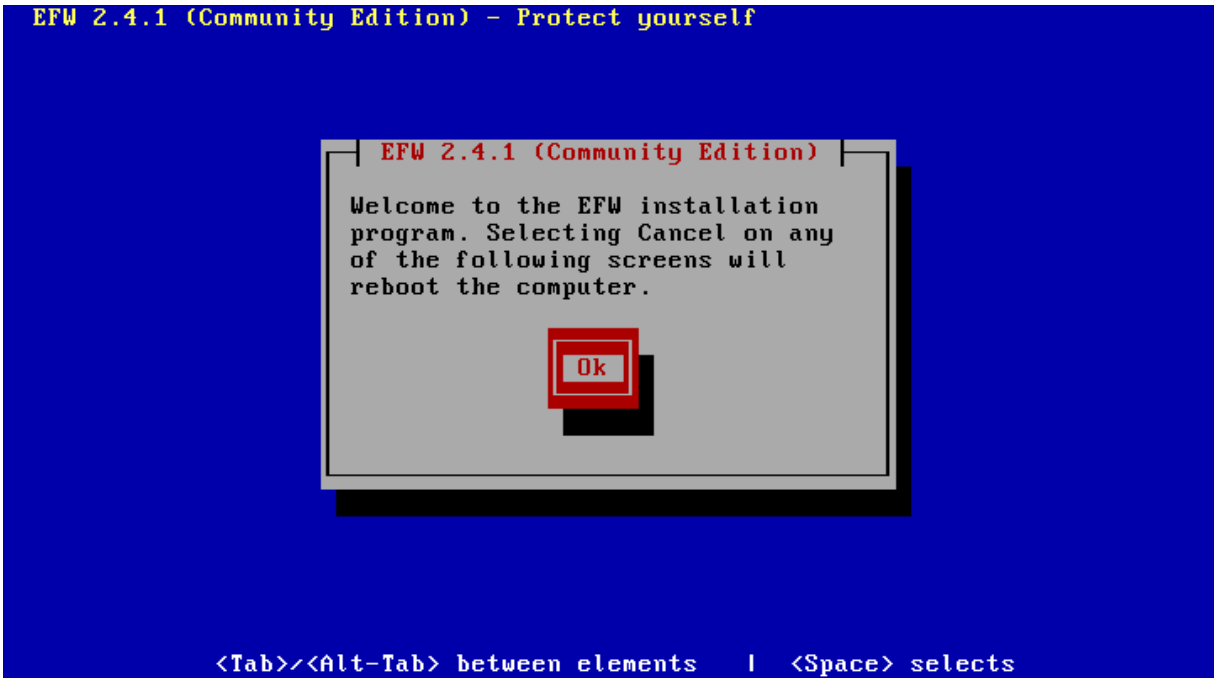
  - ✓ Endian tourne sur une machine dédiée (utilise tout le contenu du disque).
  - ✓ Caractéristiques minimales : processeur i386, 64Mo de RAM et 300Mo de disque dur.
  - ✓ Plus de RAM peut être nécessaire pour les fonctionnalités proxy web ou la détection d'intrusion, …
  - ✓ Deux cartes réseau 10/100 Mb/s
  - ✓ Un lecteur de CDROM permet une installation aisée d'Endian mais, vous pouvez installer Endian à partir du réseau via le protocole HTTP.
  - ✓ Un lecteur de disquette n'est pas obligatoire mais se révèle utile pour la création de sauvegarde et la restauration de votre configuration.
  - ✓ Endian peut également être installé sur une carte Compact Flash



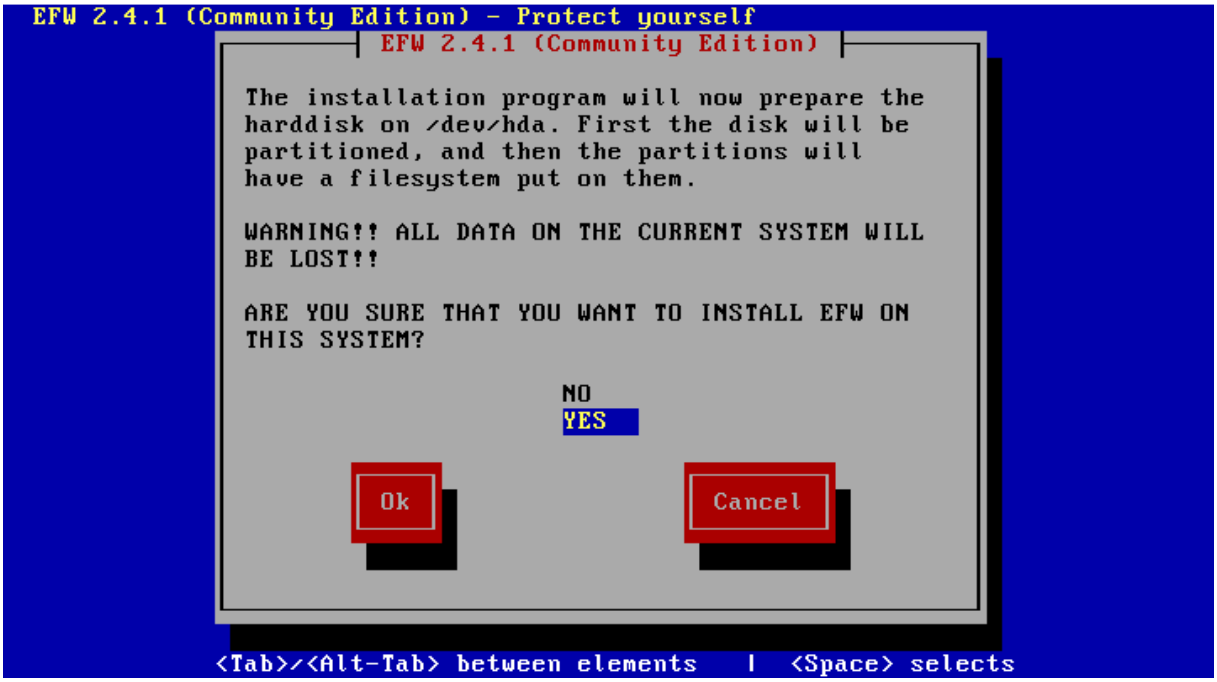
- Tapez sue entrée pour procéder à l'installation



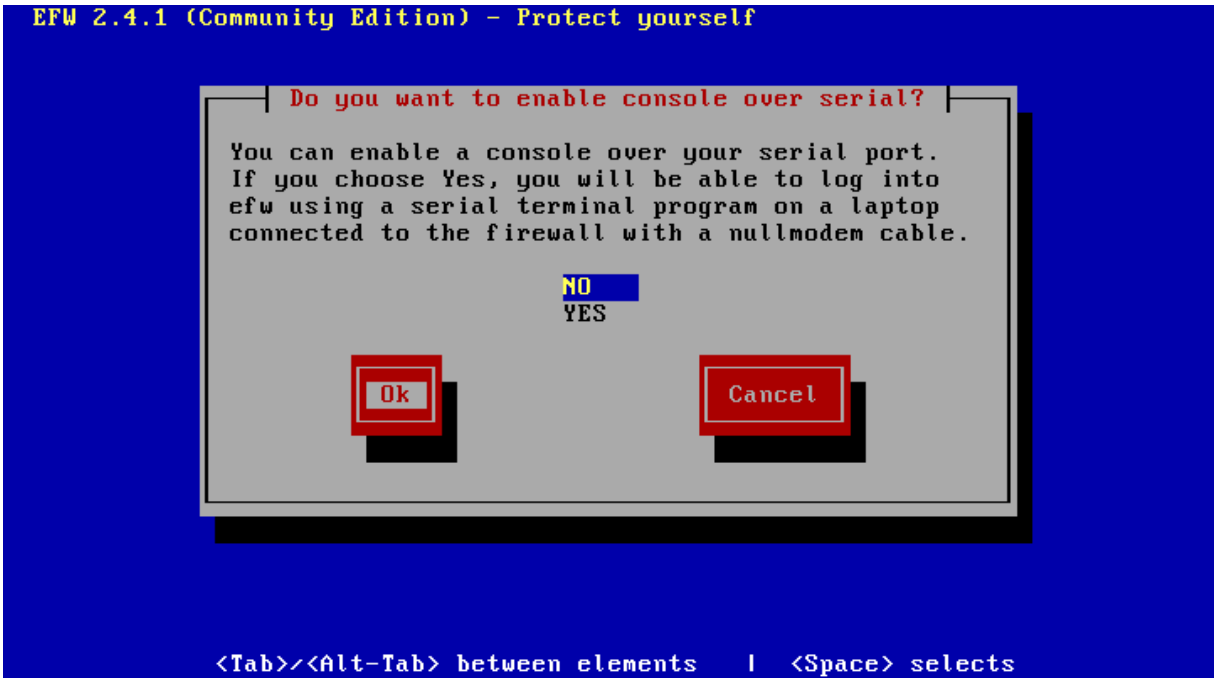
- Choisissez la langue



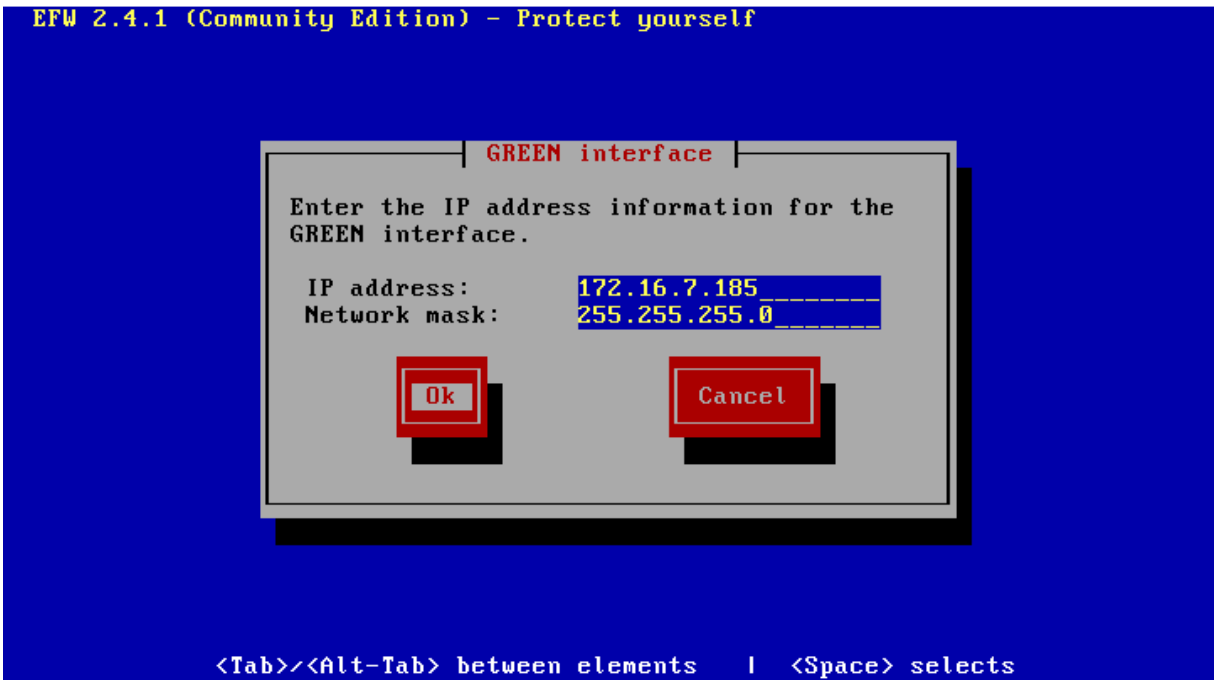
- Cliquez sur « Ok »



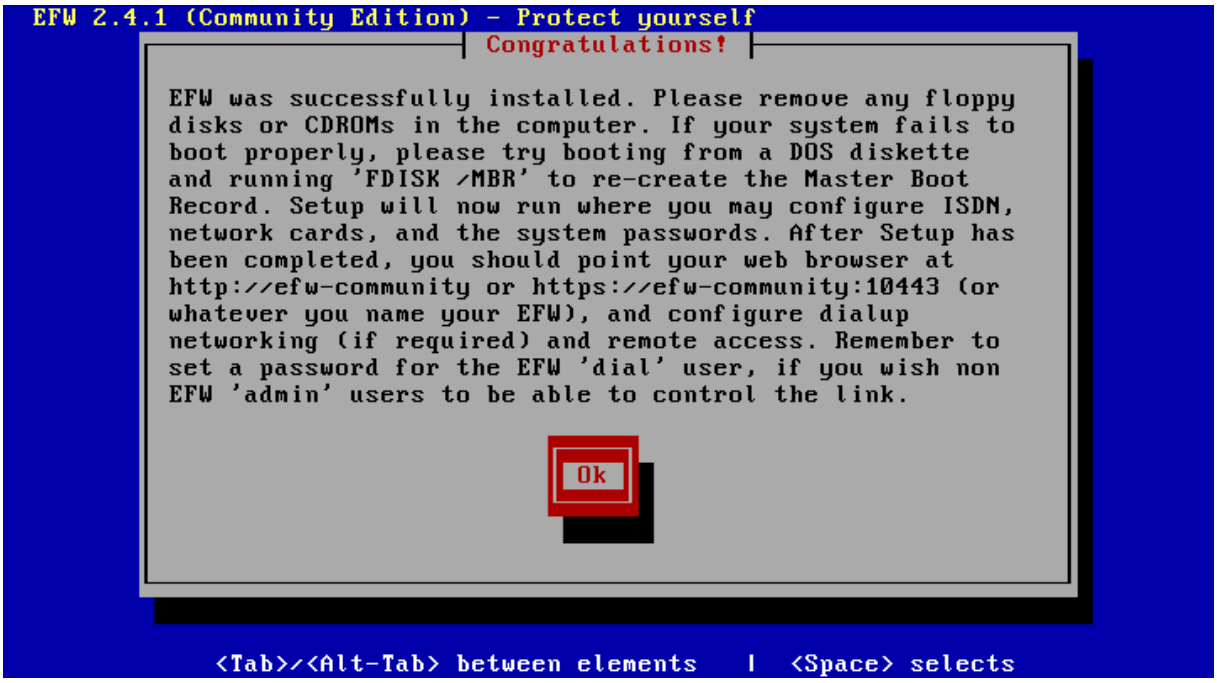
- Endian vous demande la confirmation pour formater les partitions existantes et procédez à l'installation.



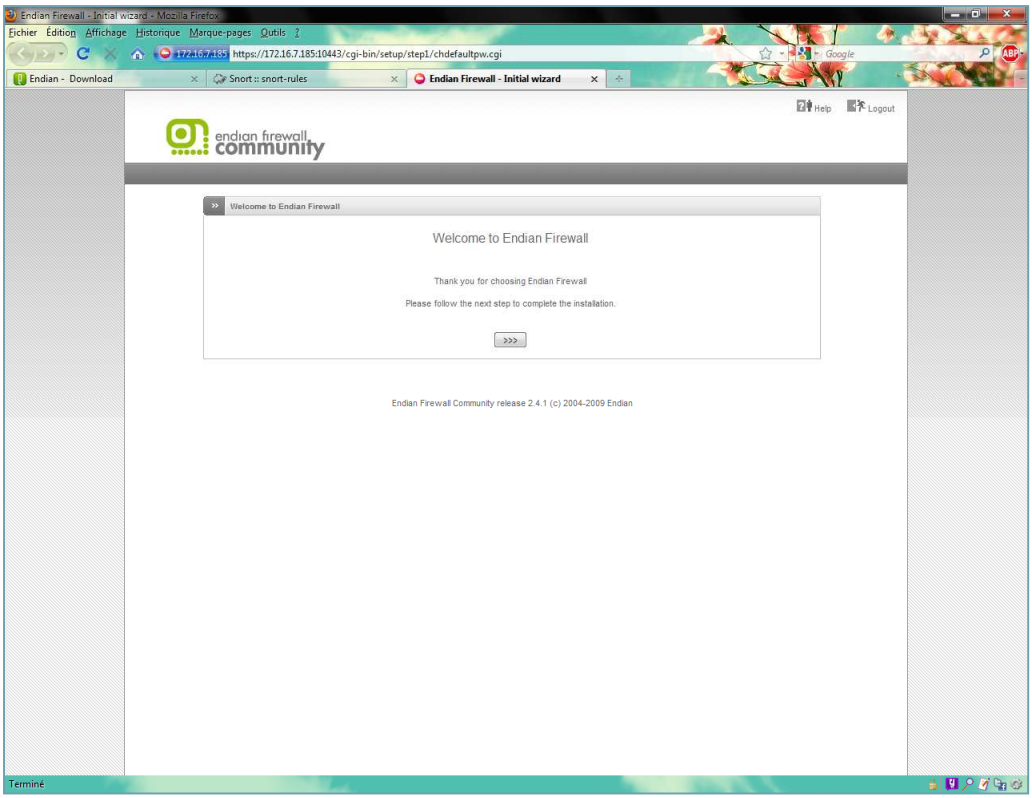
-

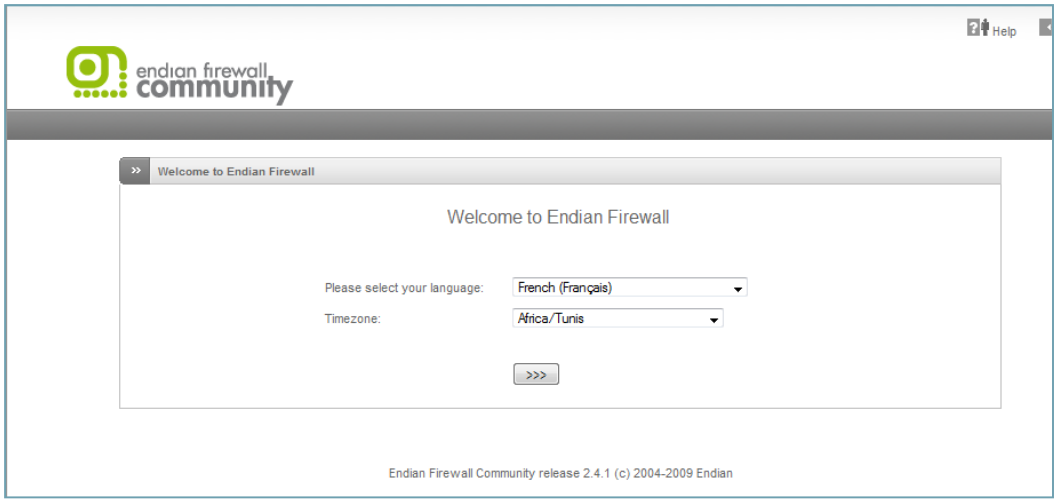


- Tapez l'adresse de la carte réseau verte (celle du réseau local)

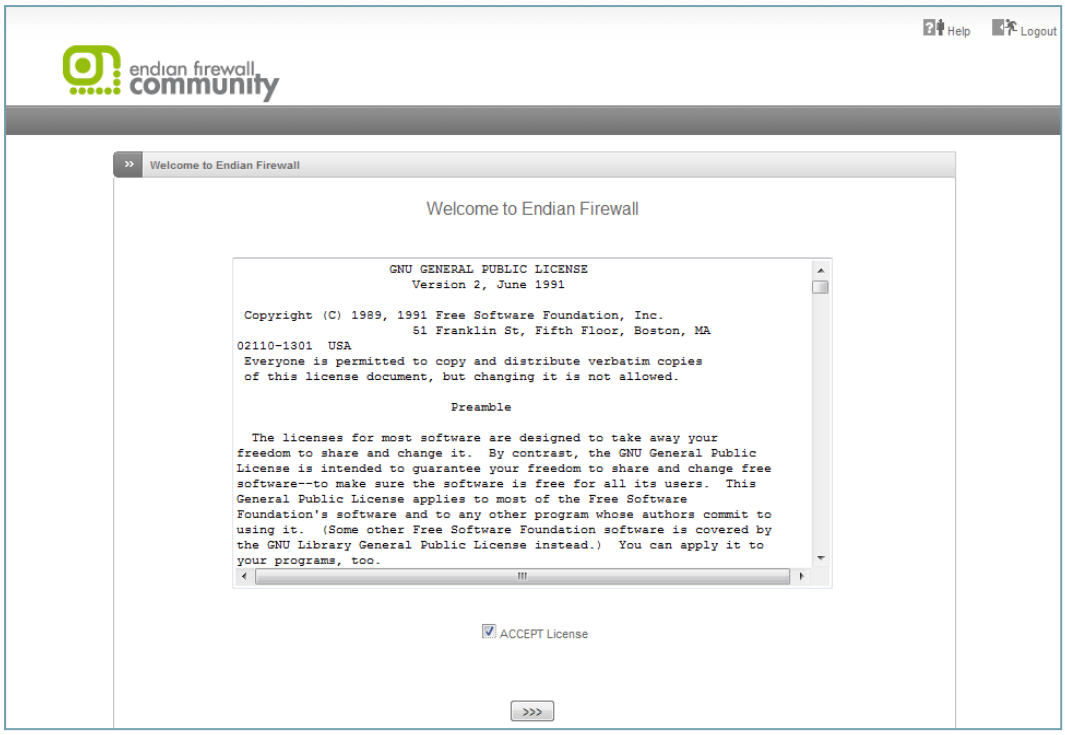


- L'installation d'EFW est terminé cliquez sur « Ok ».
- Une fois l'installation d'Endian Firewall terminé il reste encore à finaliser l'installation via l'interface web. Pour cela lancez un navigateur web et tapez :
    - http://<l'@IPd'endian>
    - https:// <l'@IPd'endian:10443>
- Vous allez être redirigé vers l'interface suivante:

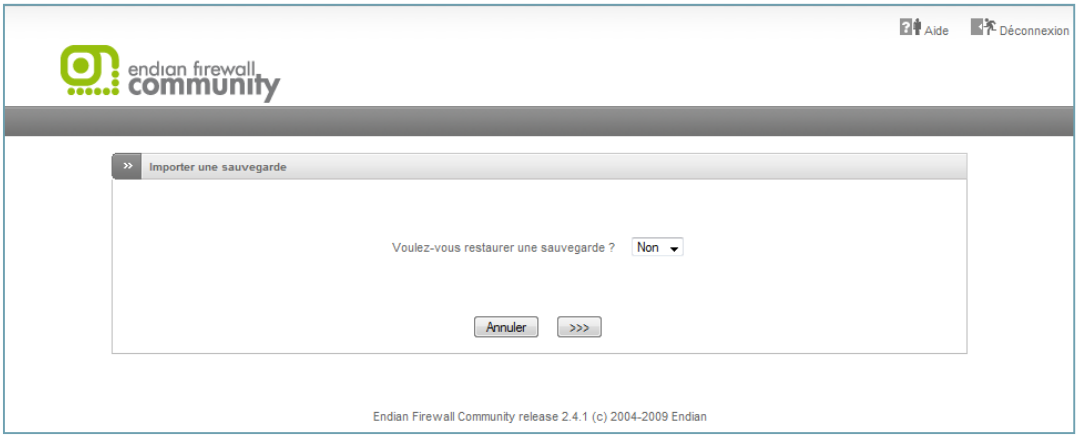




- Choisissez la langue

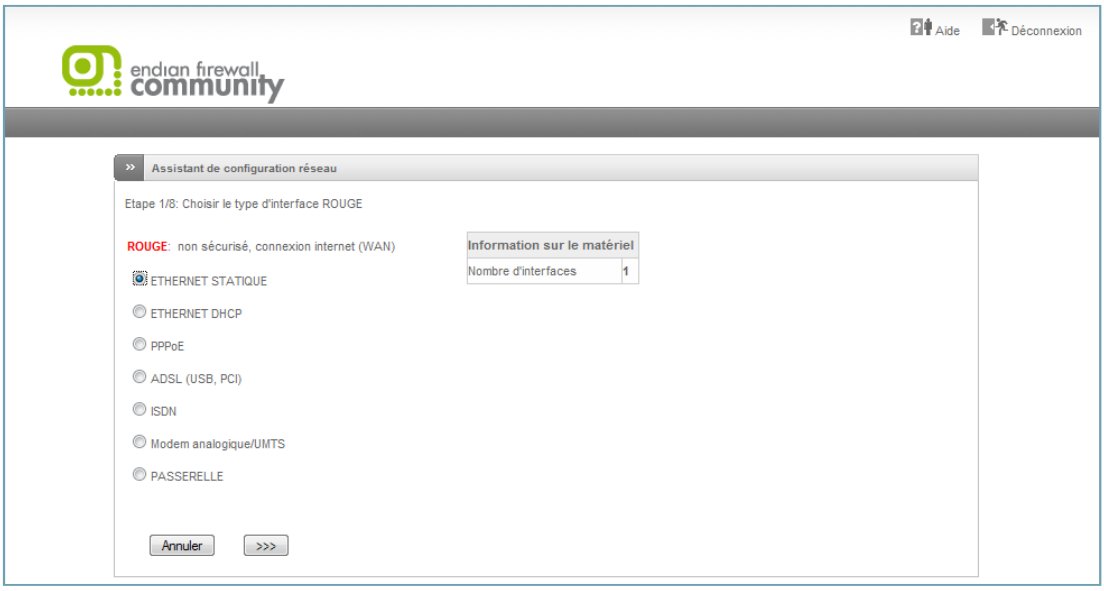


- Faites accepter la License



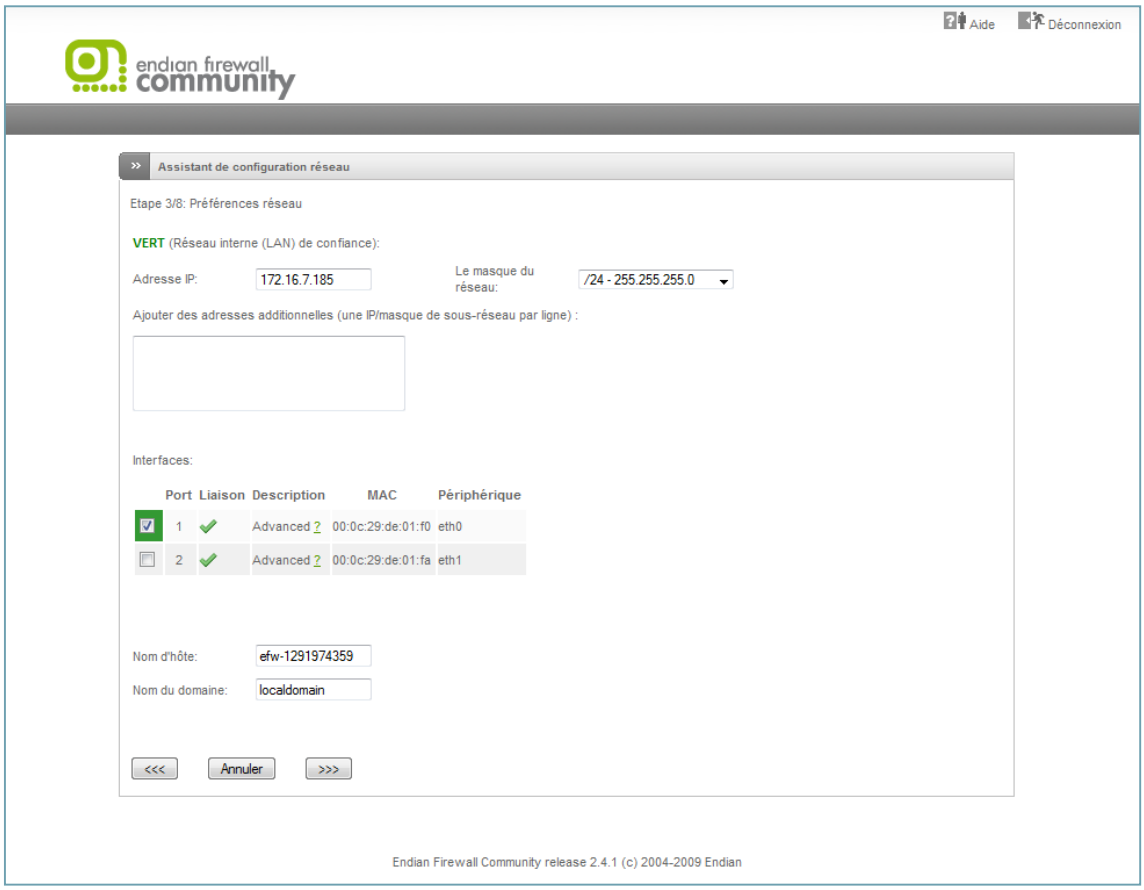
- Cette option est utile en cas ou vous voulez restaurer le système qui a été sauvegardé en restaurant un fichier de sauvegarde de configuration qui a été sauvegardé au paravent. Dans notre cas, choisissez « non » puisqu'il s'agit d'une première installation.

- Choisissez les mots de passe du compte « admin » pour l'interface web et du compte « root » pour se connecter en mode terminal sur le système.

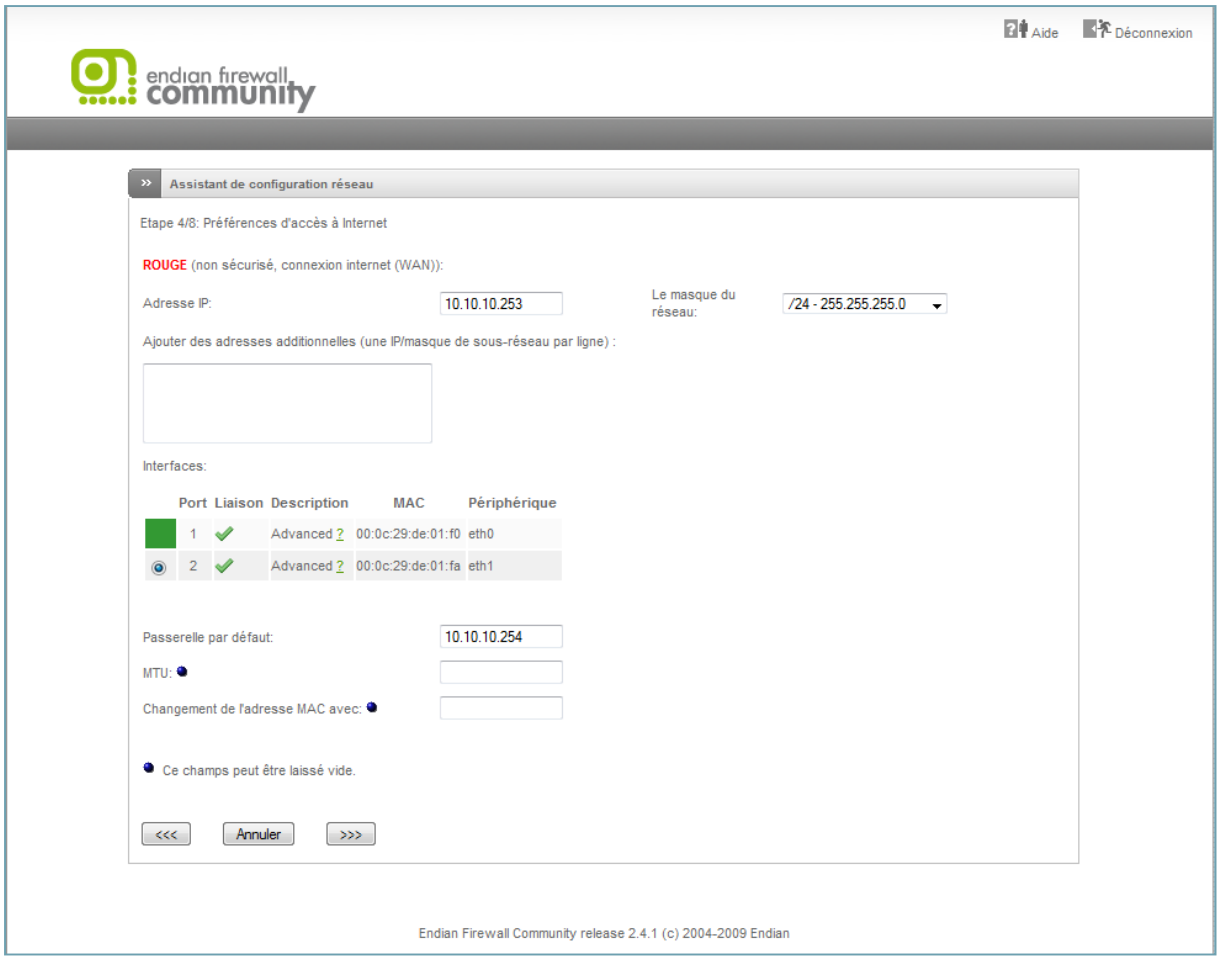


- Choisissez le type d'interface rouge (WAN), dans notre cas c'est une interface Ethernet statique.

- Si vous allez définissez une zone orange pour le DMZ ou une zone bleue pour le wifi. De même dans notre cas il s'agit d'un simple firewall entre deux zones vert (Lan) et rouge (WAN).
- Vérifiez l'adresse de l'interface verte.

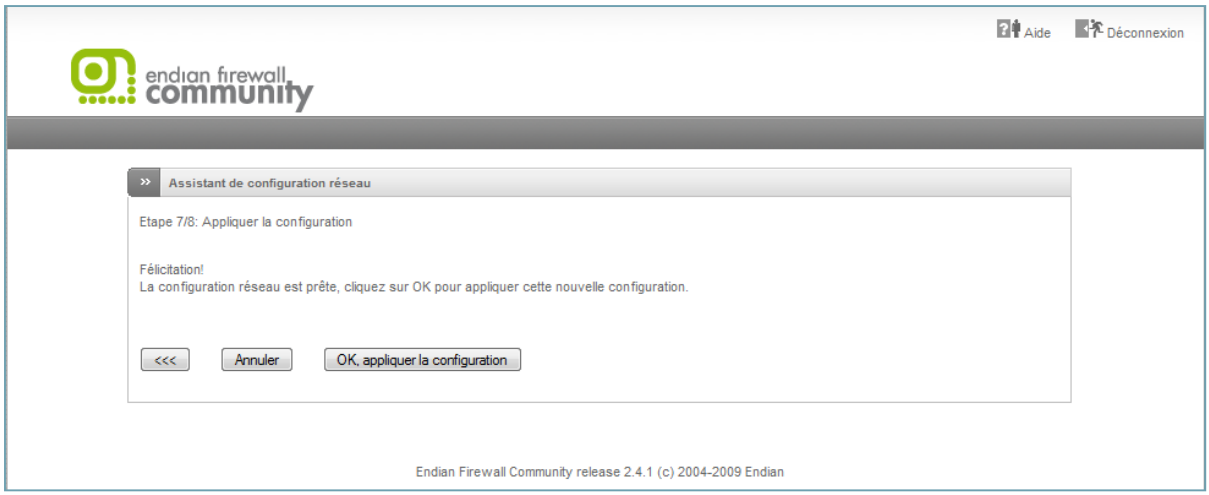


- Sélectionnez l'interface rouge et la associer son adresse et sa passerelle.

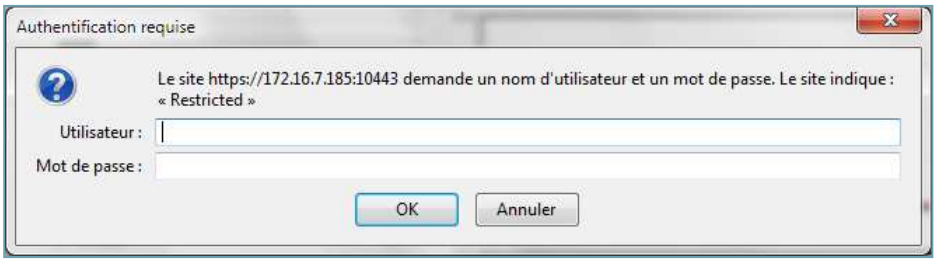


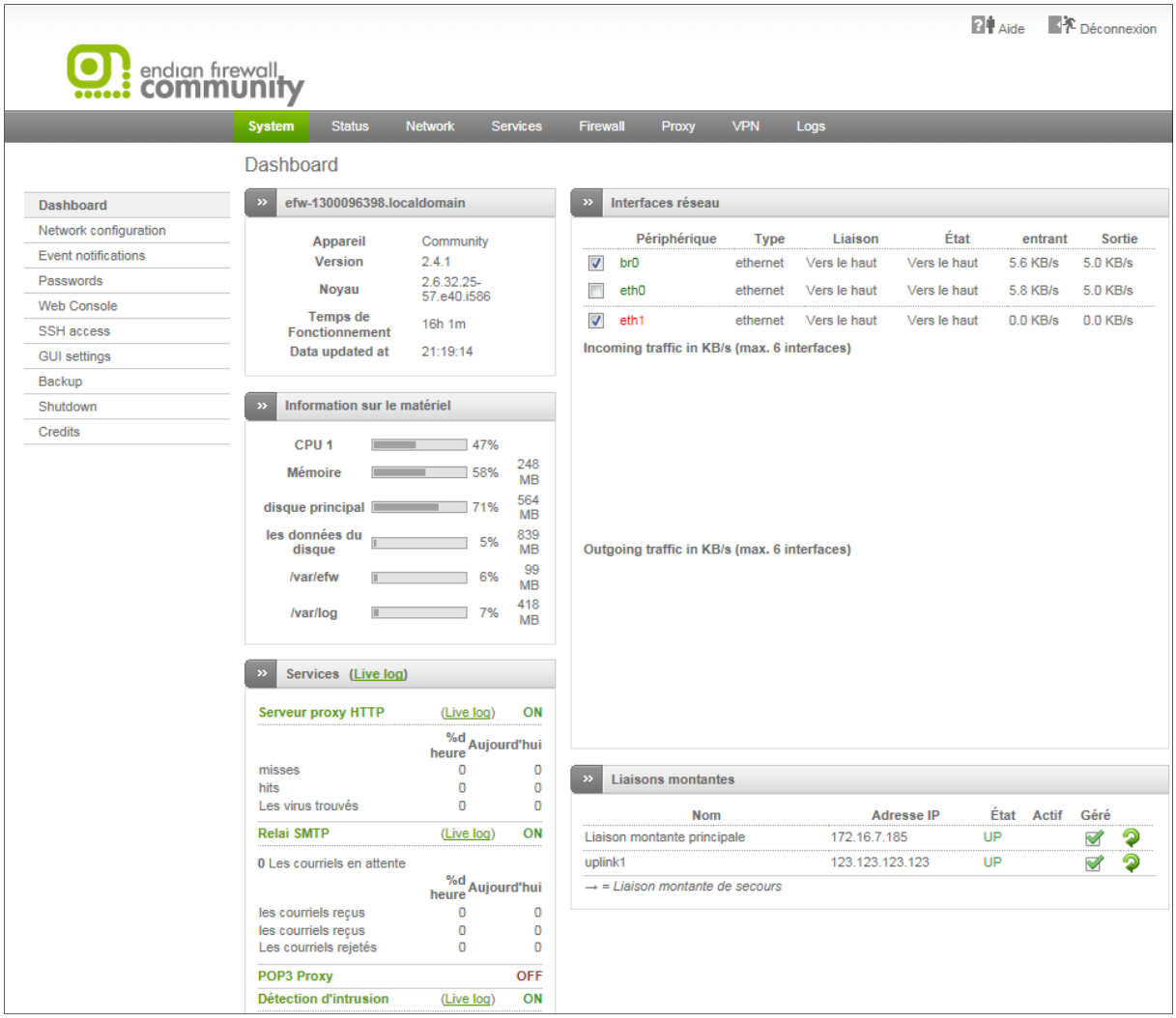
- Configurez votre DNS

- Appliquez la configuration



- Reconnectez-vous sur l'interface web d'Endian avec un login « admin » et le mot de passe que vous avez lui associé si dessus.





Voici le tableau de bord d'UTM Endian

3. Configuration des différents services d'Endian firewall :

3.1. Le menu « system » :

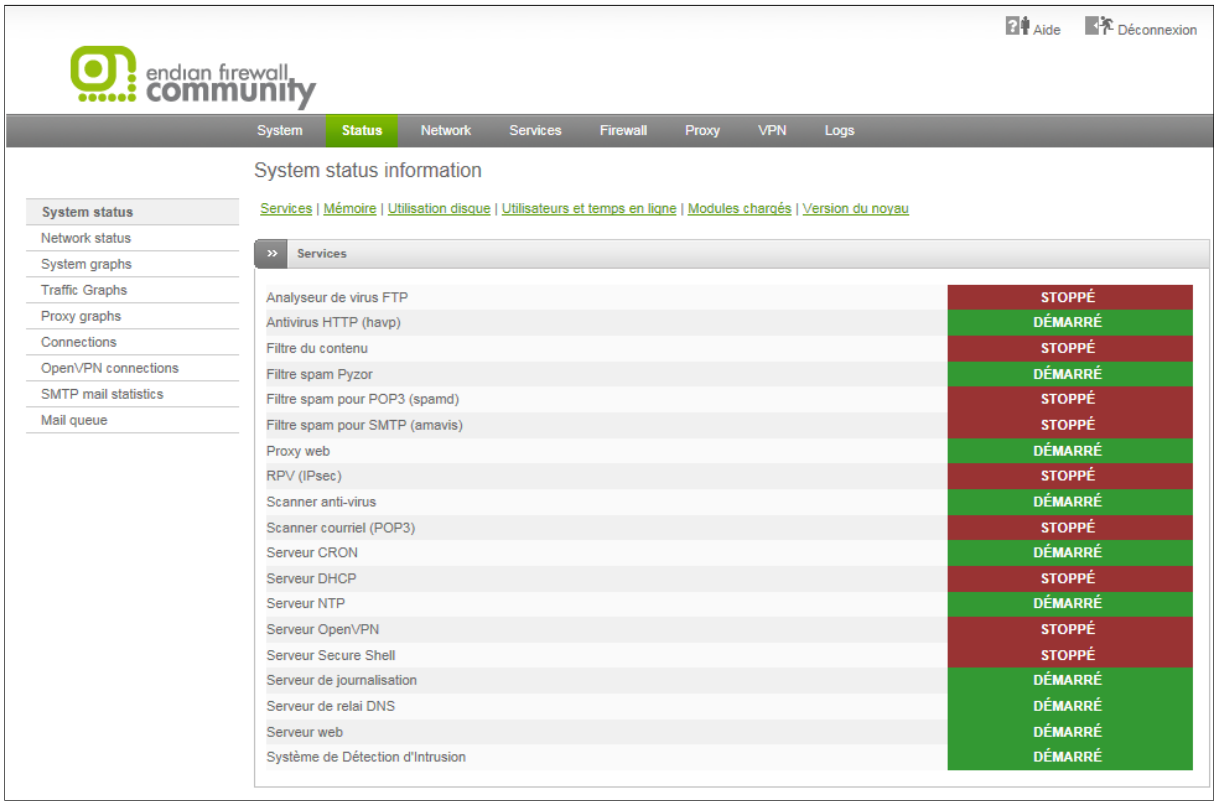
Cette section permet d'afficher toute information concernant le système et la configuration du réseau et il vous donne la main de reconfigurer le réseau.

3.2. Le menu « status » :

Cette section permet d'afficher :

- L'état du système (les services, mémoire, utilisation disque, modules chargé…).
- L'état du réseau ainsi que les graphs du trafic réseau.
- Il surveille les connexions établies par iptables ainsi que par openvpn s'il fonctionne.

- Les statistiques des emails SMTP si la passerelle antivirale est fonctionnelle.

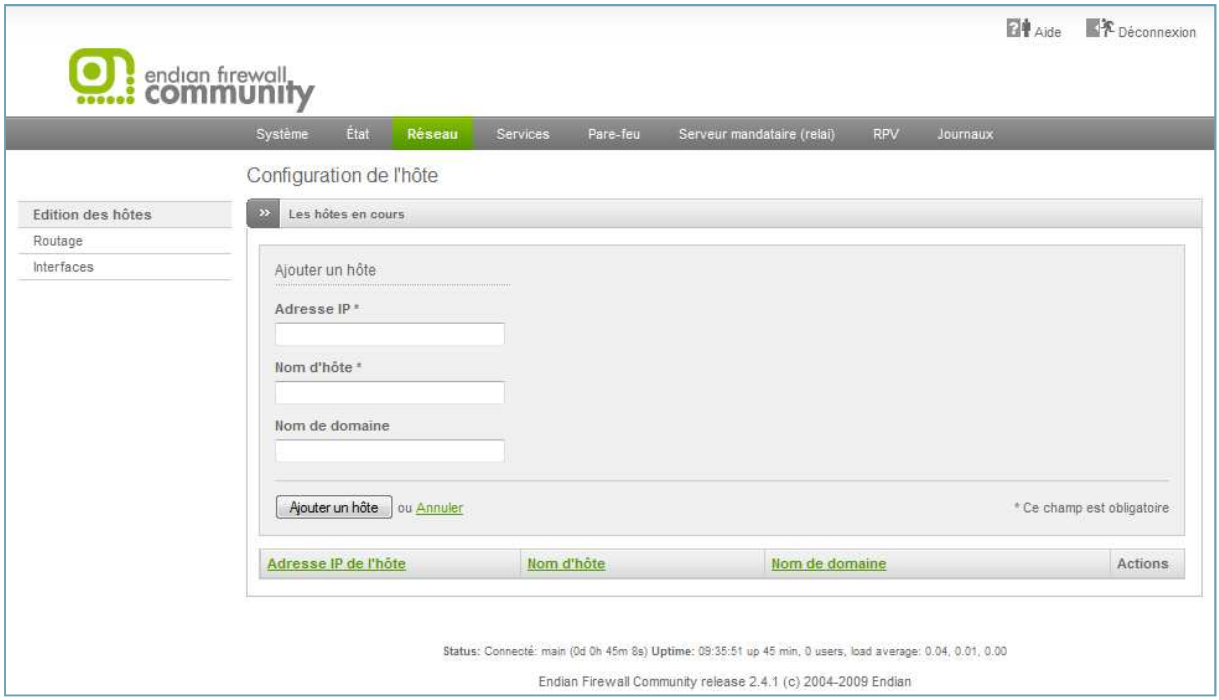


3.3. Le menu « réseau » :

Ce menu contient trois onglets :

- Edition des hôtes :

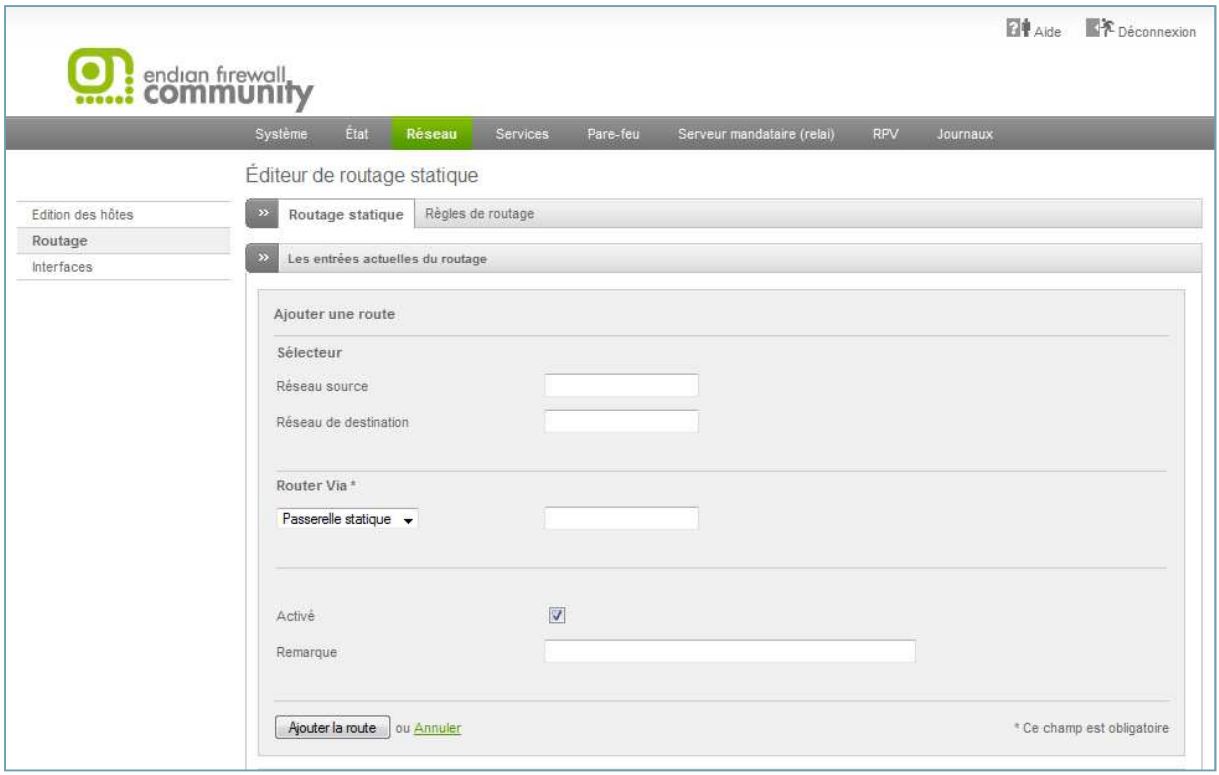
Endian contient un serveur DNS cache (dnsmasq) qui vérifie le fichier hôte du système pour le nom de look-up. Dans cette section, vous pouvez définir une entrée de l'hôte personnalisé qui sera alors résolu pour tous les clients.



❖ Routage :

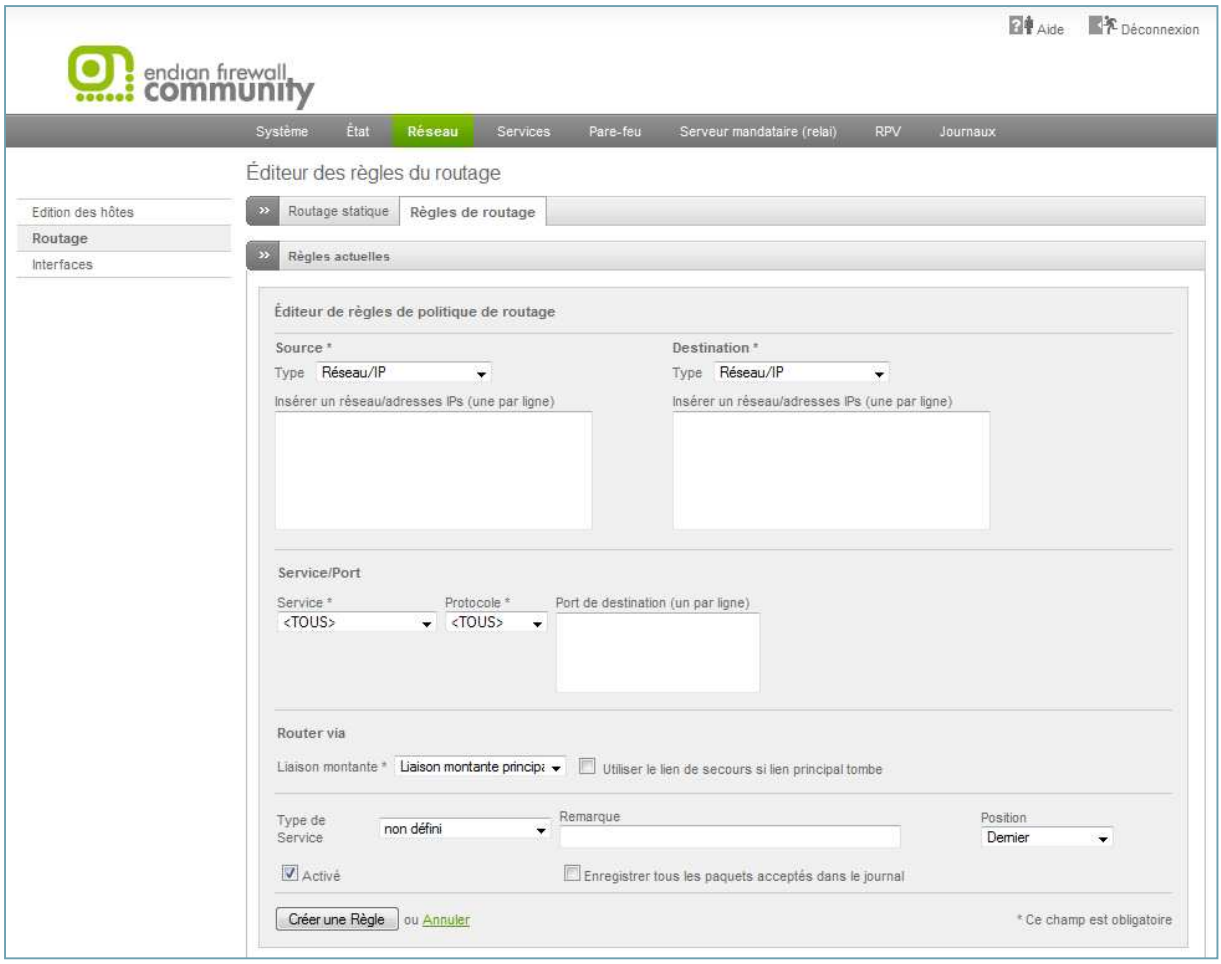
- Routage statique :

Permet d'associer des adresses de réseau spécifiques avec des passerelles données ou uplink (liaison montante). Cliquez sur le lien Ajouter une nouvelle règle pour spécifier une règle de routage statique.



- Règles de routage :

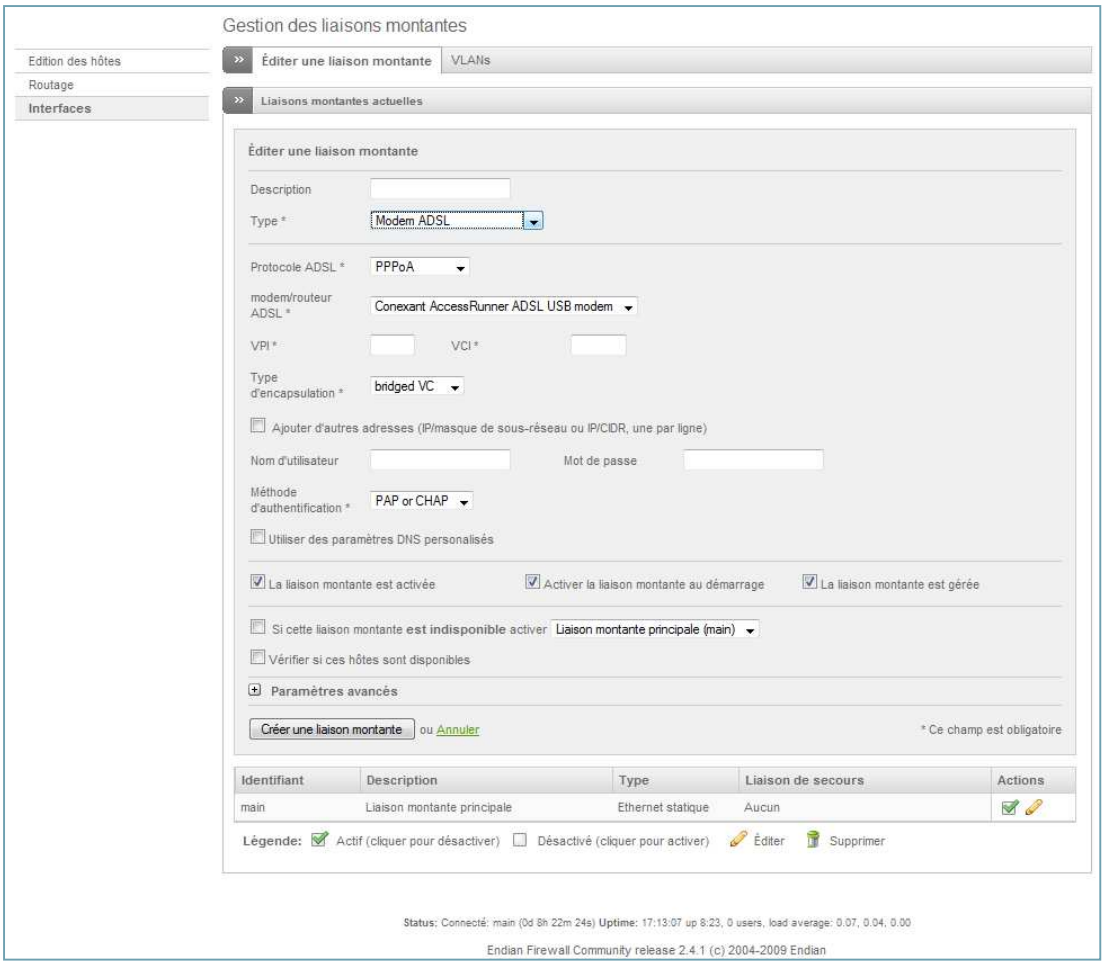
Permet d'associer des adresses de réseau spécifiques, des ports de service et des protocoles avec des uplinks donnés.



❖ Interface :

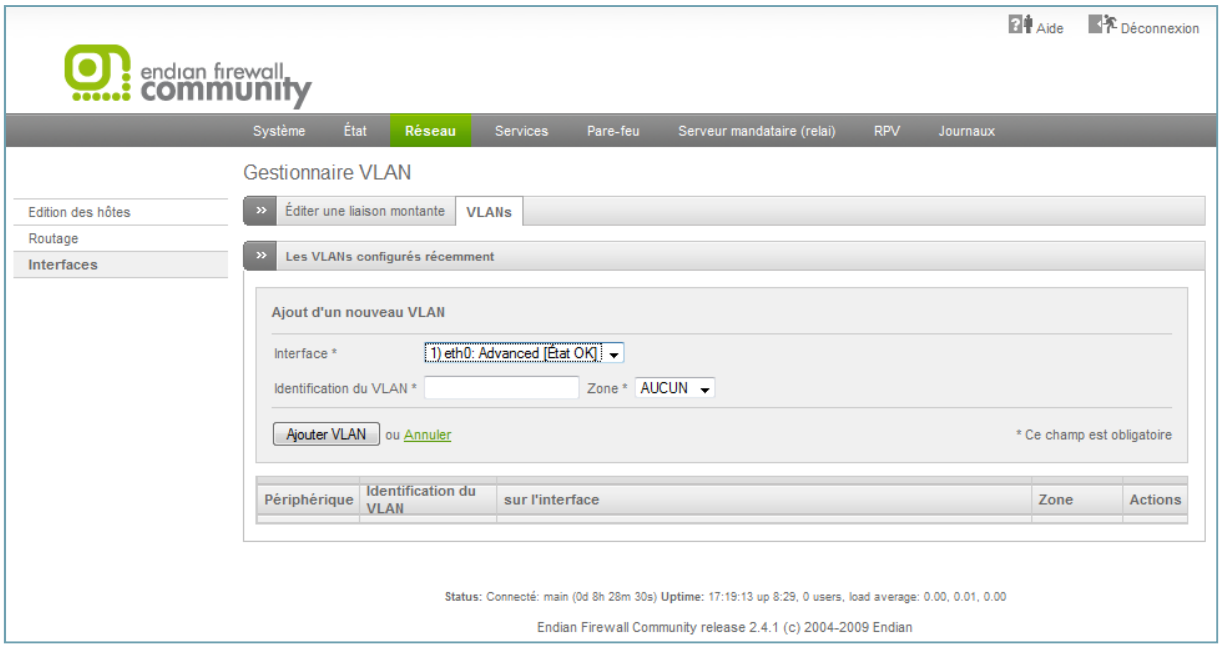
- Editer une liaison montante :

Des Uplinks supplémentaires peuvent être définies en cliquant sur l'onglet éditeur d'Uplink: choisir le type de liaison montante, puis remplir le formulaire spécifique de ce dernier.



- VLANs :

Les réseaux locaux virtuels (VLAN) peuvent être définis en cliquant sur l'onglet VLAN. Le support des vlans par Endian offre l'idée d'associer les « vlans ids » avec les zones du firewall.



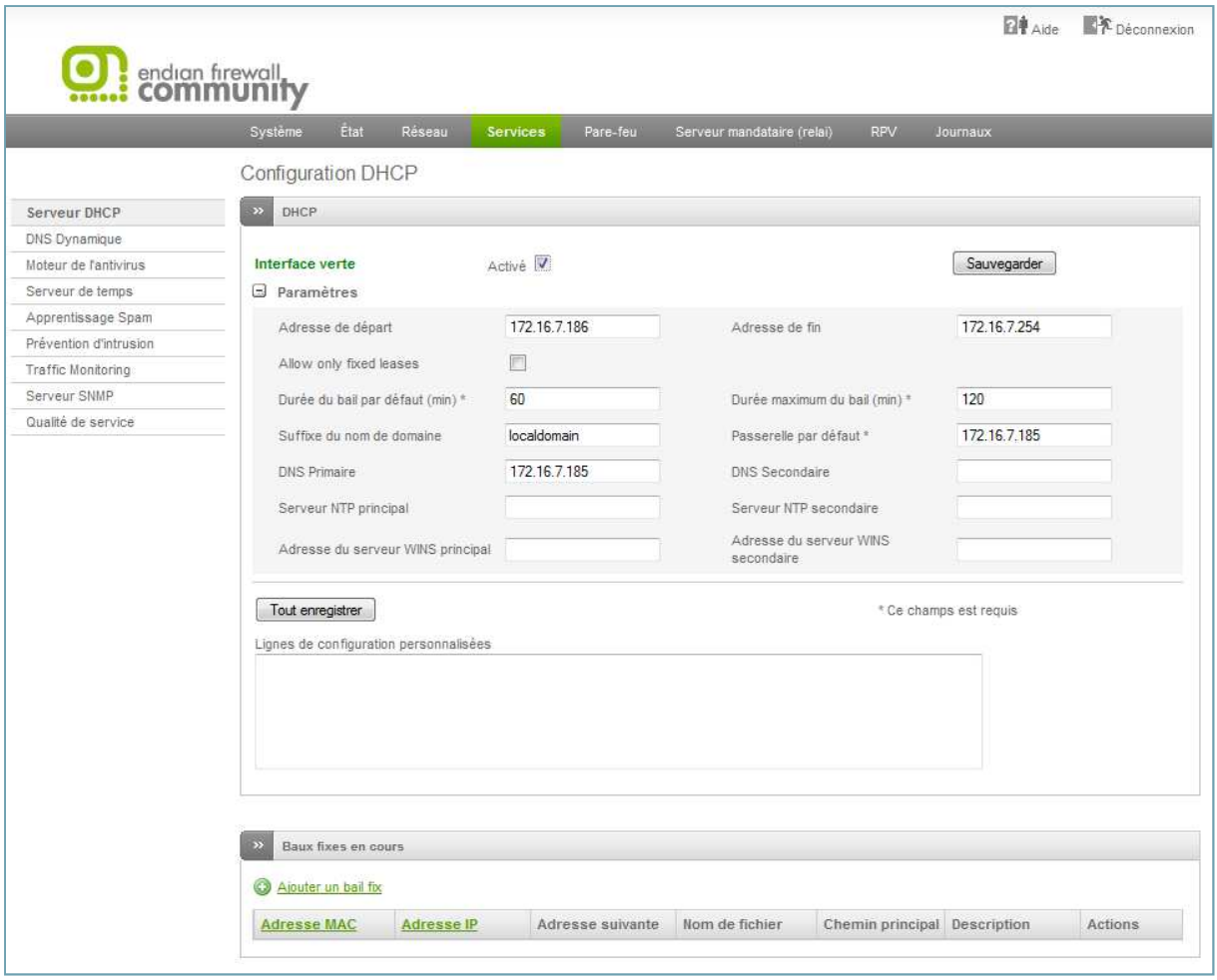
3.4. LE MENU « SERVICES » :

Endian peut fournir un certain nombre de services utiles qui peuvent être configurés dans cette section. En particulier, il s'agit des services utilisés par le proxy tel que : l'antivirus clamav. Ainsi que l'IDS « snort ».

Voici donc la liste des services qui peuvent être activés via Endian:

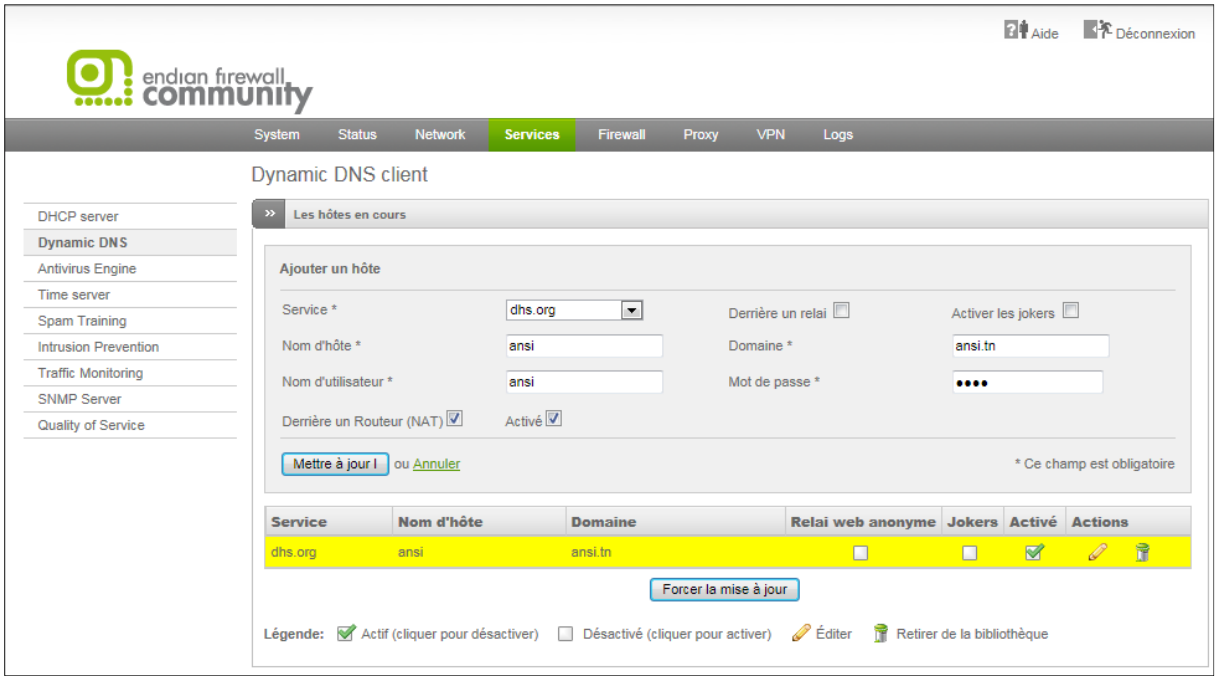
a) Serveur DHCP :

- Le protocole DHCP (Dynamics Host Configuration Protocol) vous permet de contrôler la configuration des adresses IP de tous vos périphériques réseau via votre d'Endian UTM de façon centralisée.
- Quand un client (hôte client ou une imprimante en réseau, etc) se joint à votre réseau, il obtiendra automatiquement une adresse IP valide à partir d'une plage d'adresses et d'autres paramètres de la fonction DHCP. Le client doit être configuré pour utiliser DHCP.
- Vous pouvez choisir d'offrir ce service aux clients de la zone verte, ou comprennent des dispositifs sur le ORANGE (DMZ) ou BLEU (WLAN) zone en cochant les cases à cocher qui sont étiquetés.



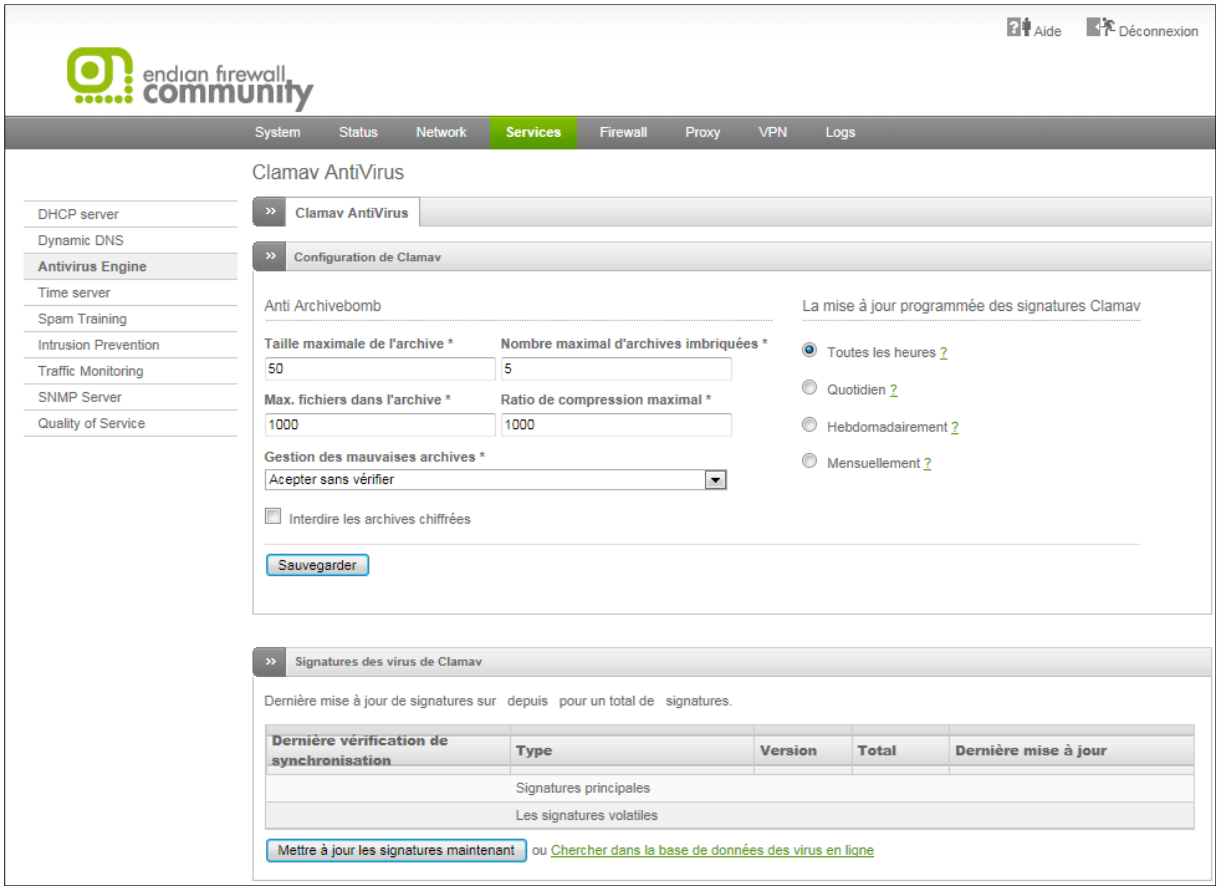
b) DNS dynamique:

- Les fournisseurs de DNS Dynamique comme «DynDNS» offre un service qui permet d'affecter un nom de domaine à des adresses IP. Cela fonctionne même avec des adresses qui se changent dynamiquement, tels que ceux offerts par des connexions ADSL.
- Chaque fois que le changement d'adresse IP est effectué, la mise à jour doit être activement propagé au fournisseur de DNS dynamique.
- Endian UTM contient un client DNS dynamique pour les 14 fournisseurs différents, si elle est activée, il se connectera automatiquement au fournisseur de DNS dynamique et de lui demander la nouvelle adresse IP après chaque changement d'adresse.



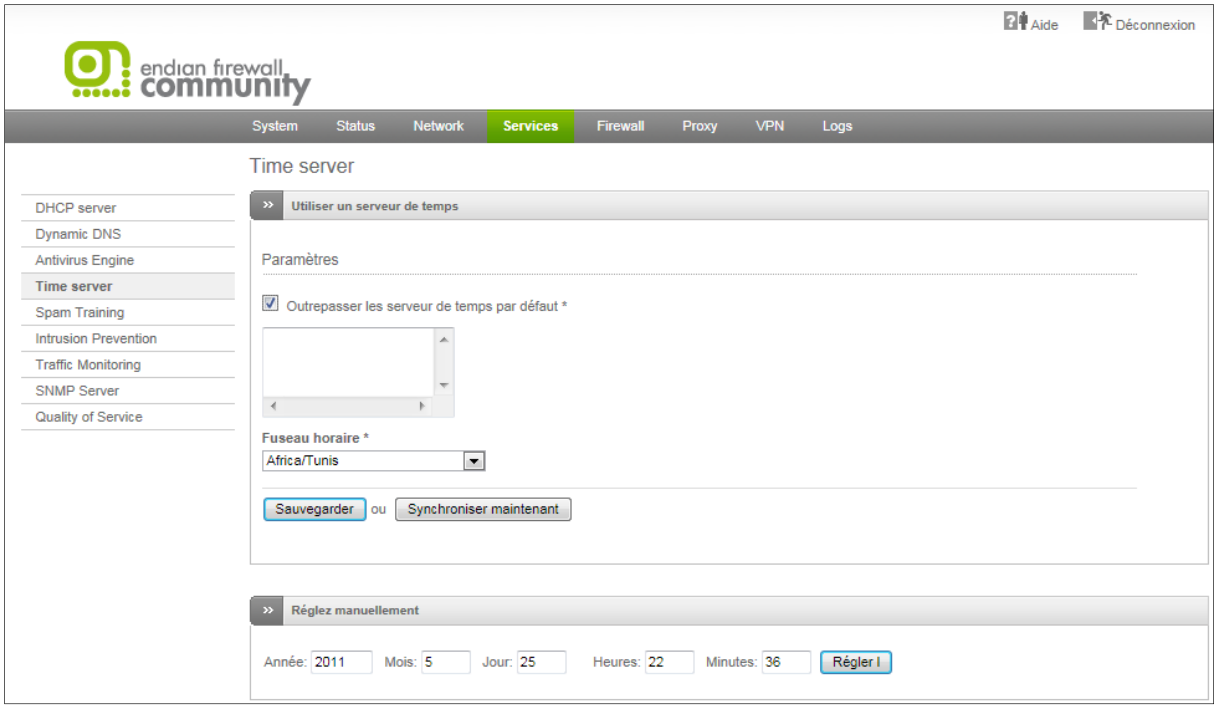
c) Moteur de l'antivirus:

- Ce module vous permet de configurer la manière dont ClamAV devrait traiter les archives et la synchronisation des mises à jour de signature.
- Le démarrage de mise à jour se fait manuellement, ainsi vous pouvez vérifier quand la dernière mise à jour a été effectuée.



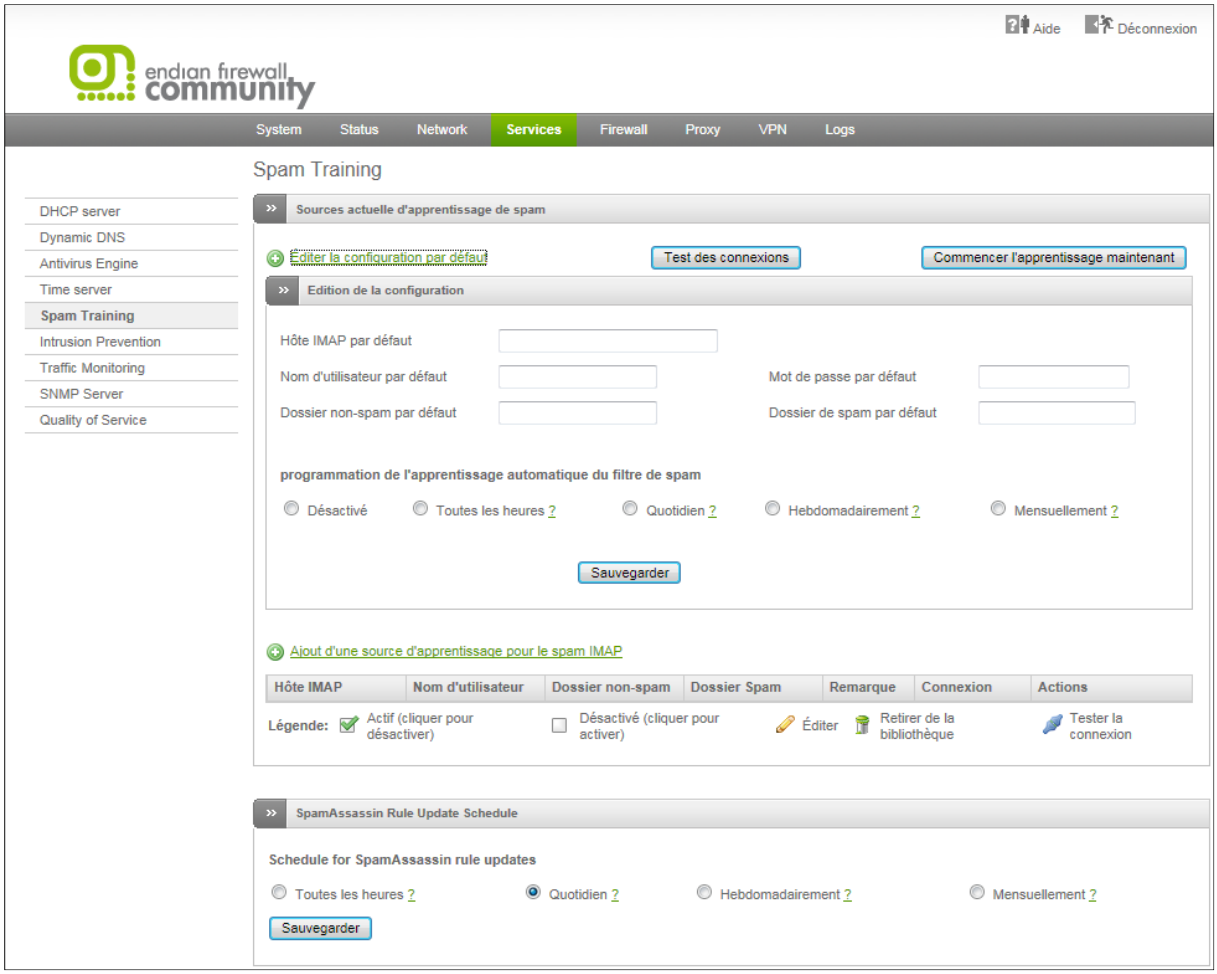
d) Serveur de temps:

- Endian conserve l'heure du système synchronisé au serveur de temps sur internet en utilisant le protocole NTP (Network Time).
- Un certain nombre de serveur de temps sur internet sont préconfigurés et utilisé par le système.
- Cliquez sur les serveurs NTP Remplacer par défaut pour spécifier vos propres serveurs de temps manuellement. Cela peut être nécessaire si vous utilisez une configuration qui ne permet pas à Endian d'accéder à Internet. Ces hôtes doivent être ajoutés un par ligne.



e) Apprentissage Spam:

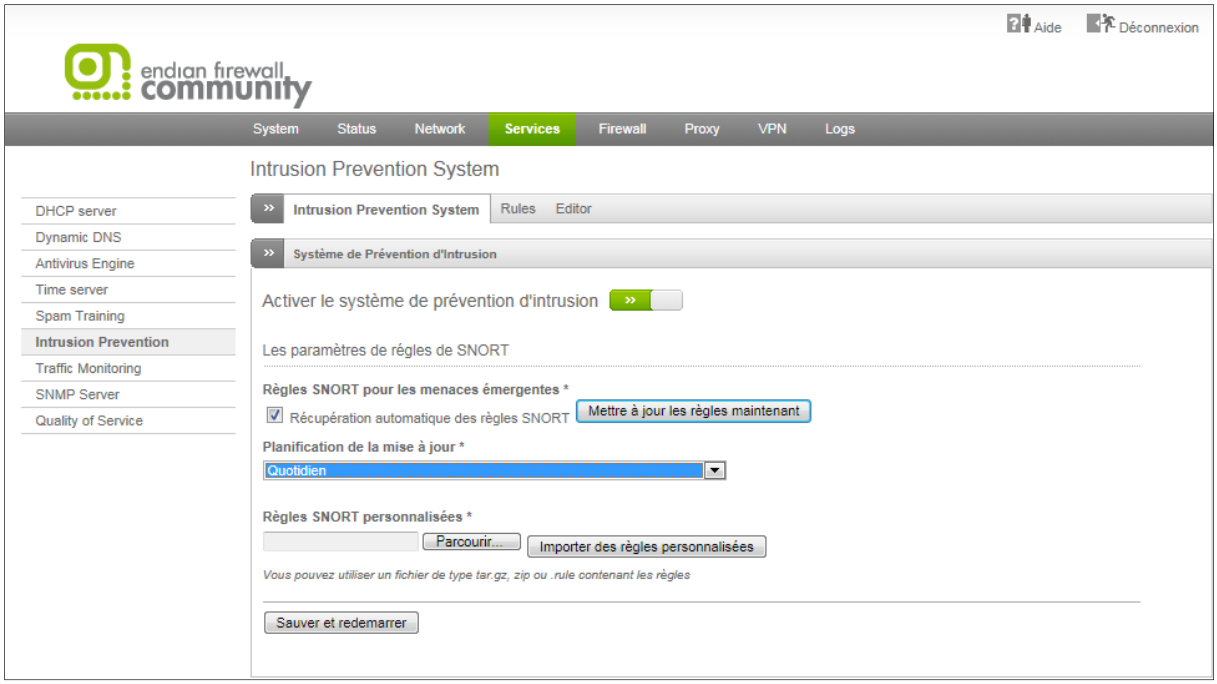
- SpamAssassin peut être configuré pour faire un apprentissage automatique des e-mails qui sont classés comme spams. Pour être en mesure d'apprendre, il doit se connecter à un serveur IMAP et vérifier avec les blacklists de spam existants.



f) Prévention d'intrusion:

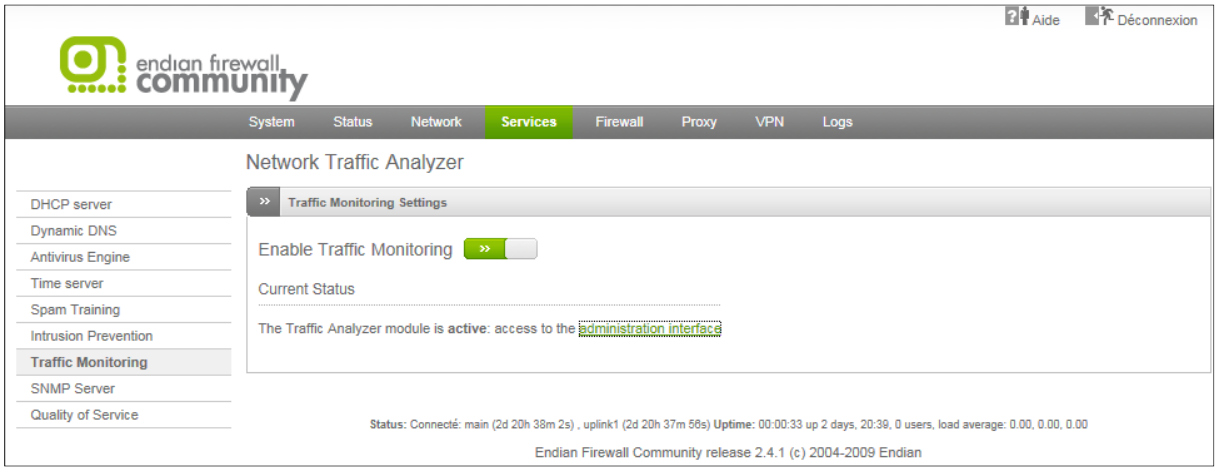
- Endian inclut comme moteur de détection d'intrusion système « snort ».
- Vous pouvez l'activez seulement sur la zone verte.
- Pour les règles de snort, soit :

  - D'activer l'option de récupération des règles automatiquement et de planifier les mises à jour.
  - D'importer des règles personnalisées et manuellement.



g) Traffic Monitoring:

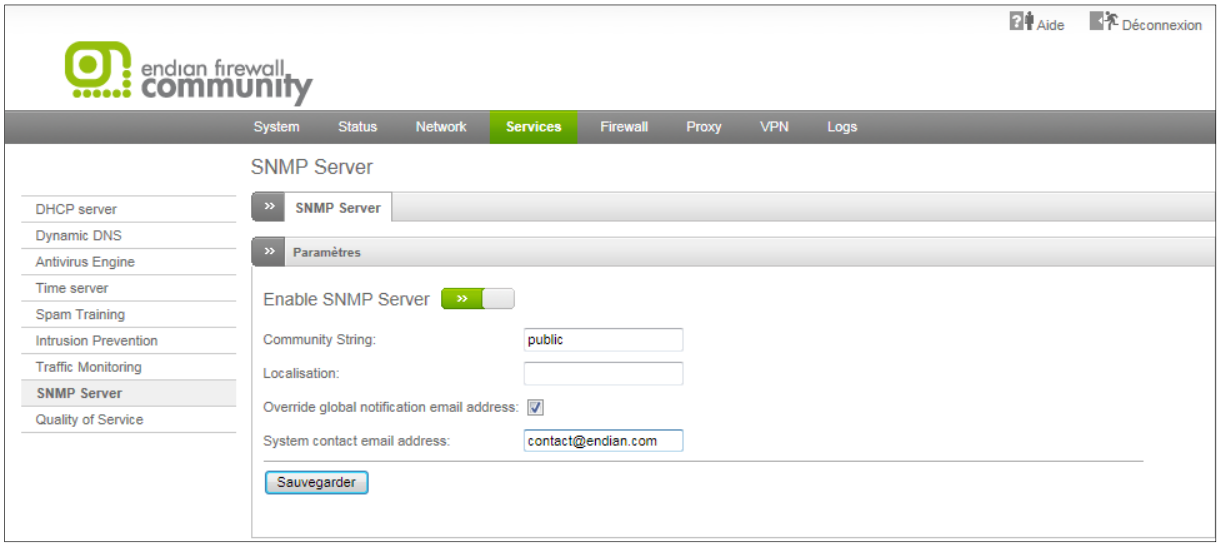
- La supervision du trafic se fait par « ntop » et peut être activée ou désactivée en cliquant sur l'interrupteur principal sur cette page.
- Une fois que la supervision du trafic est activée un lien vers l'interface d'administration de « ntop » s'affiche dans un autre onglet.
- Cette interface d'administration est assurée par « ntop » et comprend des statistiques détaillées sur le trafic réseau. Ce dernier peut être analysé par hôte, protocole, interface réseau ainsi que des autres types d'informations.



h) Serveur SNMP:

- Le Simple Network Management Protocol (SNMP) est peut être utilisé pour contrôler les différents éléments du réseau. Endian intègre un serveur SNMP.
- Si vous voulez l'activer, un peu d'options apparaîtra :

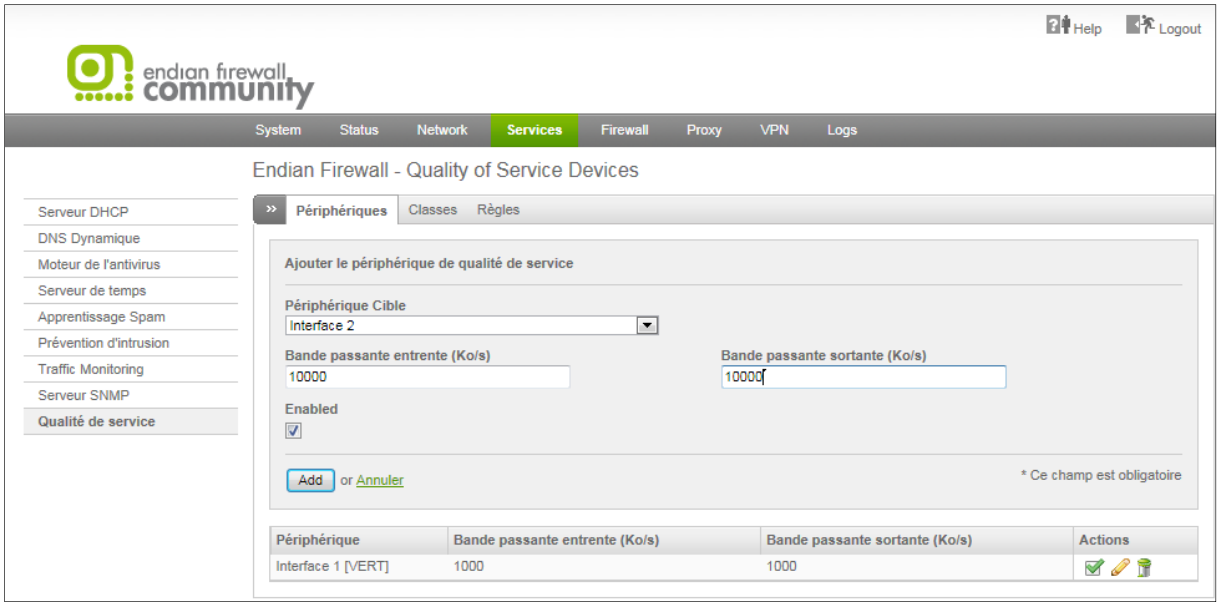
  - Community string : c'est une clé qui est nécessaire pour lire les données avec un client SNMP.
  - System contact email address : Le serveur SNMP nécessite une adresse email de l'administrateur système pour être configuré.



i) Qualité de service :

- Permet de classer par priorité le trafic IP qui passe par votre firewall en fonction du service.
- Les applications qui ont généralement besoin d'avoir la priorité sur le trafic en vrac comme les téléchargements sont des services interactifs tels que Secure Shell (SSH) ou de la voix sur IP (VoIP).
- Vous devez alors configurer :

  - Les périphériques : ajouter les périphériques (zone, interface, liaison montante, VPN IPSEC).
  - Les classes : classez les périphériques ajoutés par classe.
  - Les règles : attribuez les priorités aux différents périphériques et/ou classes déjà définis.



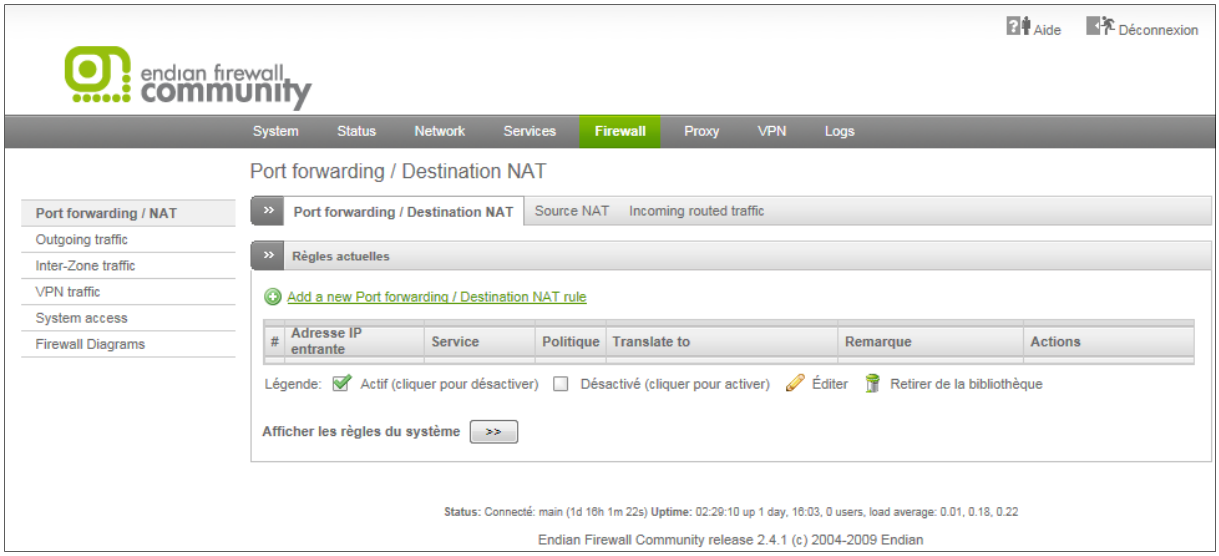
3.5. LE MENU « FIREWALL » :

Cette section vous permet de configurer les règles de votre firewall qui spécifient comment le trafic réseau sera dirigé.

Voici une liste de liens qui apparaissent sur le côté gauche de l'écran:

- Port forwarding/NAT : pour configurer la redirection des ports et le NAT (network address translation).
- Outgoing traffic : permet d'autoriser ou d'interdire le traffic sortant (vers le rouge) et le paramétrer par zone, hôte, port, etc
- Inter-Zone traffic : permet d'autoriser ou d'interdire la circulation entre les zone
- VPN traffic : afin de préciser si les hôtes se connectant via un VPN doivent être passé par le firewall.
- System Access : accorder l'accès à l'hôte Endian

a) Port forwarding/NAT:



- Destination NAT :

Destination NAT est généralement utilisé pour permettre l'accès réseau limité à partir d'un réseau non sécurisé, ou de translater certains ports à d'autres adresses. Il est possible de définir quel port de l'interface qui doit être transmis à un hôte donné et le port.

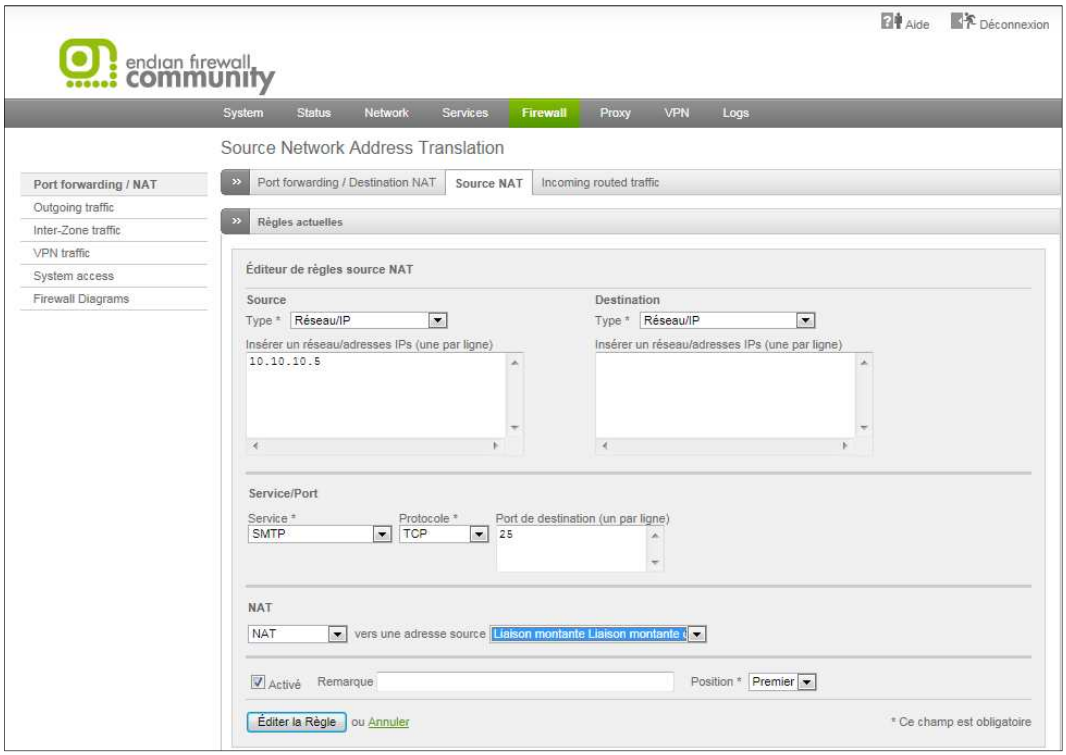
- Source NAT :

Cette section permet de définir à quel trafic sortant la Source NAT doit être appliqué. Cette dernière peut être utile dans le cas où vous avez un serveur derrière votre firewall Endian qui possède sa une adresse IP externe et vous voulez que les paquets sortants utilisent une adresse IP autre que celle de l'interface RED du pare-feu. Pour ce cas, il faut ajouter des règles NAT Source est similaire à l'ajout de règles de transfert de port.

Exemple:

1- Configuration d'un serveur SMTP fonctionne sur IP 123.123.123.123 (en supposant que 123.123.123.123 est son adresse IP externe) dans la zone démilitarisée avec NAT source.
2- Configurer votre zone « orange » que vous le souhaitez.
3- Configurer le serveur SMTP à l'écoute sur le port 25 sur un réseau IP appartenant à la zone orange.
4- Ajouter une liaison montante (uplink) avec Ethernet IP statique 123.123.123.123 à votre firewall Endian dans la section interface réseau.

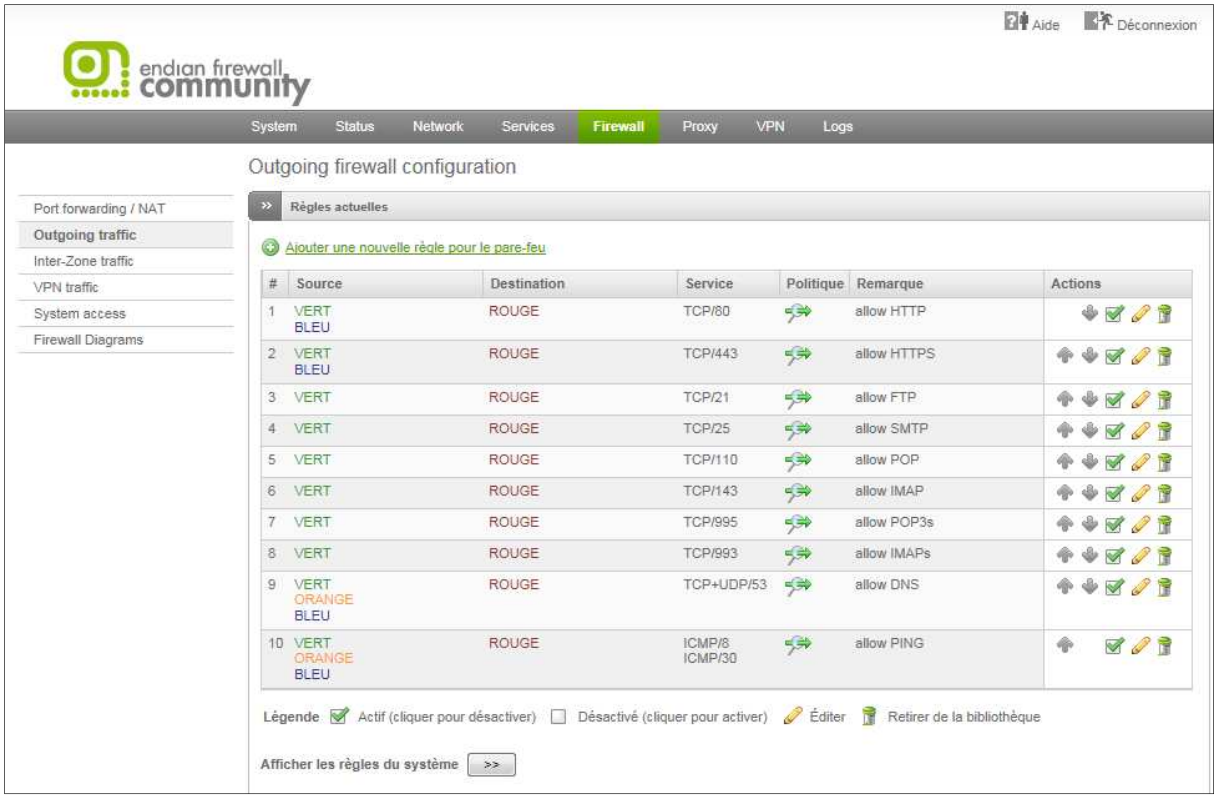
5- Ajouter une règle source NAT et spécifier, en tant qu'adresse source, l'adresse IP ORANGE du serveur SMTP. Veillez à utiliser NAT et définir la source de NAT l'adresse IP 123.123.123.123.



- Incoming routed traffic :

Avec ce module, vous pouvez rediriger le trafic qui a été acheminé par le biais de votre firewall Endian. Ceci est très utile si vous avez plus d'une adresse IP externe et que vous souhaitez utiliser certains d'entre eux dans votre DMZ sans avoir à utiliser NAT.

b) Outgoing traffic

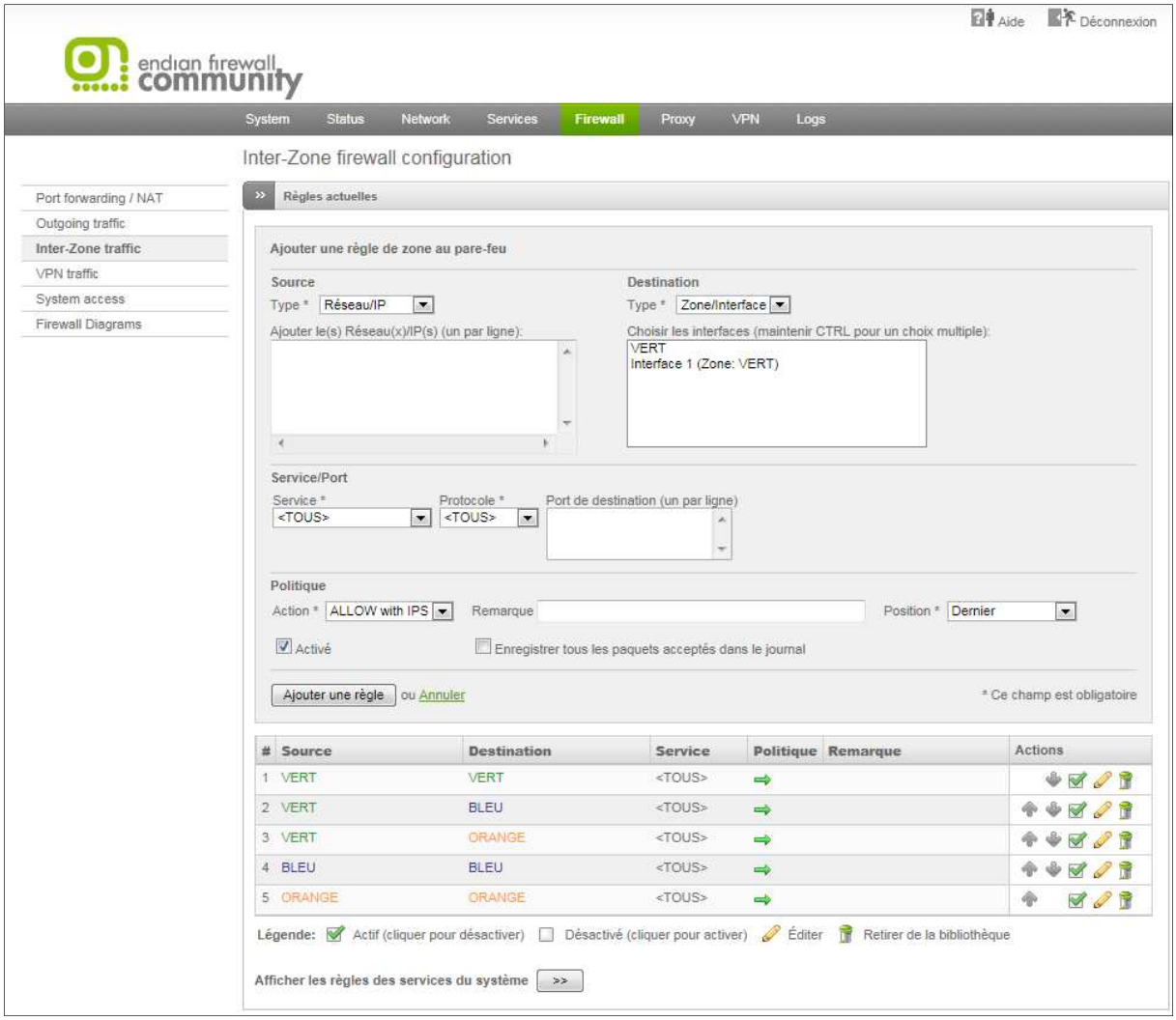


Endian est préconfiguré avec un ensemble de règles, qui autorisent le trafic sortant de la zone verte en ce qui concerne les services les plus courants (HTTP, HTTPS, FTP, SMTP, POP, IMAP, POP3s, IMAP, DNS, ping). Tous les autres services sont bloqués par défaut. De même, l'accès à HTTP, HTTPS, DNS et ping est autorisée à partir de la zone bleue (WLAN) alors que DNS et ping sont autorisés de la zone orange (DMZ). Tout le reste est interdit par défaut.

Dans ce module, vous pouvez activer/désactiver, modifier ou supprimer des règles en cliquant sur l'icône appropriée sur la côté droite de la table. Vous pouvez également ajouter vos propres règles en cliquant sur le lien Ajouter un nouveau règle pare-feu.

NB : l'ordre des règles est important: la première règle correspondant au paquet décide si ce dernier est autorisé ou non, peu importe combien de règles de correspondance pourrait le suivre.

c) Inter-Zone traffic:



Cette section vous permet de mettre en place des règles qui déterminent la façon dont le trafic peut circuler entre les différentes zones réseau, à l'exclusion de la zone rouge. Endian est fourni avec un ensemble simple de règles préconfigurées:

- Le trafic est autorisé de la zone verte à toute autre zone (orange et bleu) et la circulation est autorisée dans chaque zone.
- Tout le reste est interdit par défaut.

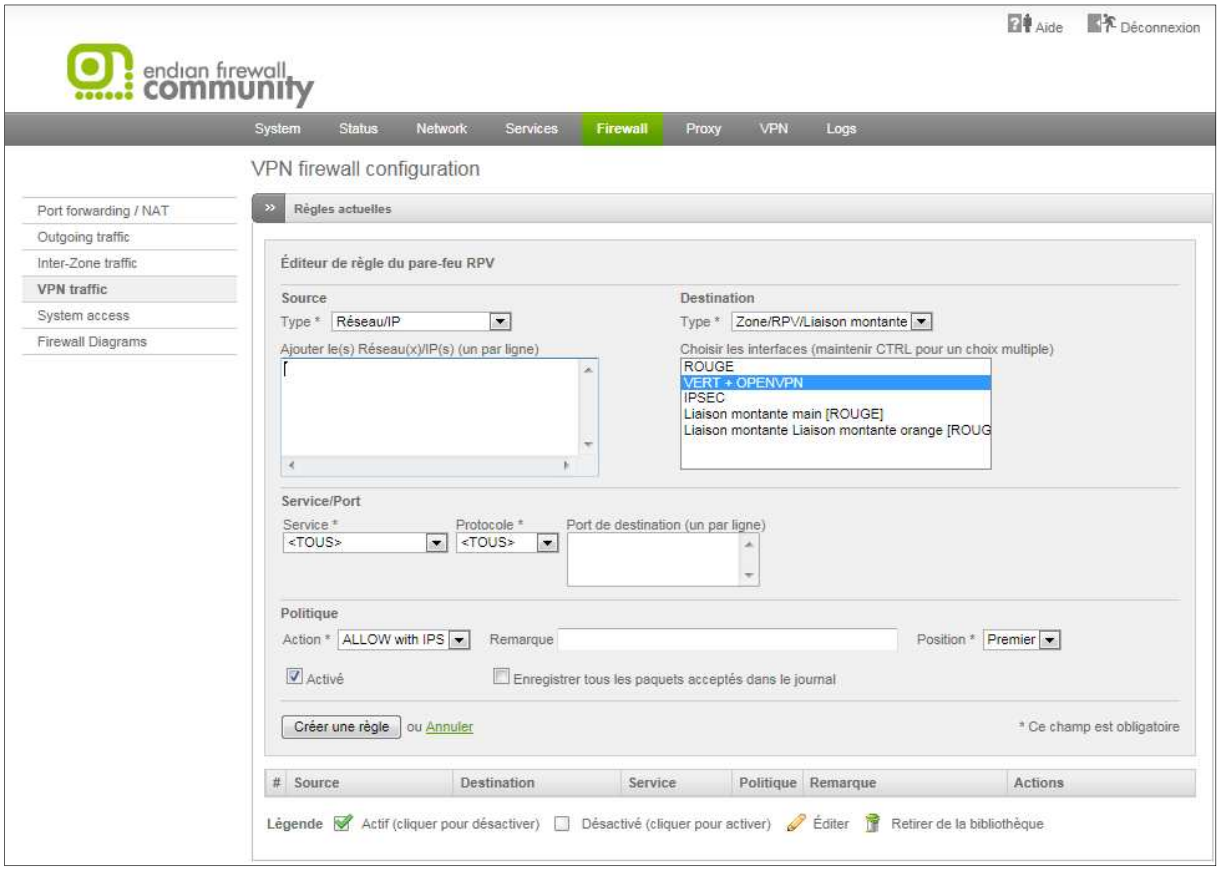
Similaire au module « Outgoing traffic », vous pouvez activez/désactivez, modifier ou supprimer des règles en cliquant sur l'icône appropriée sur la côté droite du tableau.

Vous pouvez également ajouter vos propres règles en cliquant sur le lien « Ajouter une règle de pare-feu Inter-Zone »

Le firewall Inter-Zone peut être activés/désactivés dans son ensemble en utilisant l'option « Activer le pare-feu Inter-Zone ».

NB : Lorsqu'il est désactivé, tout le trafic est autorisé entre toutes les zones autres que la zone rouge.

d) VPN traffic :



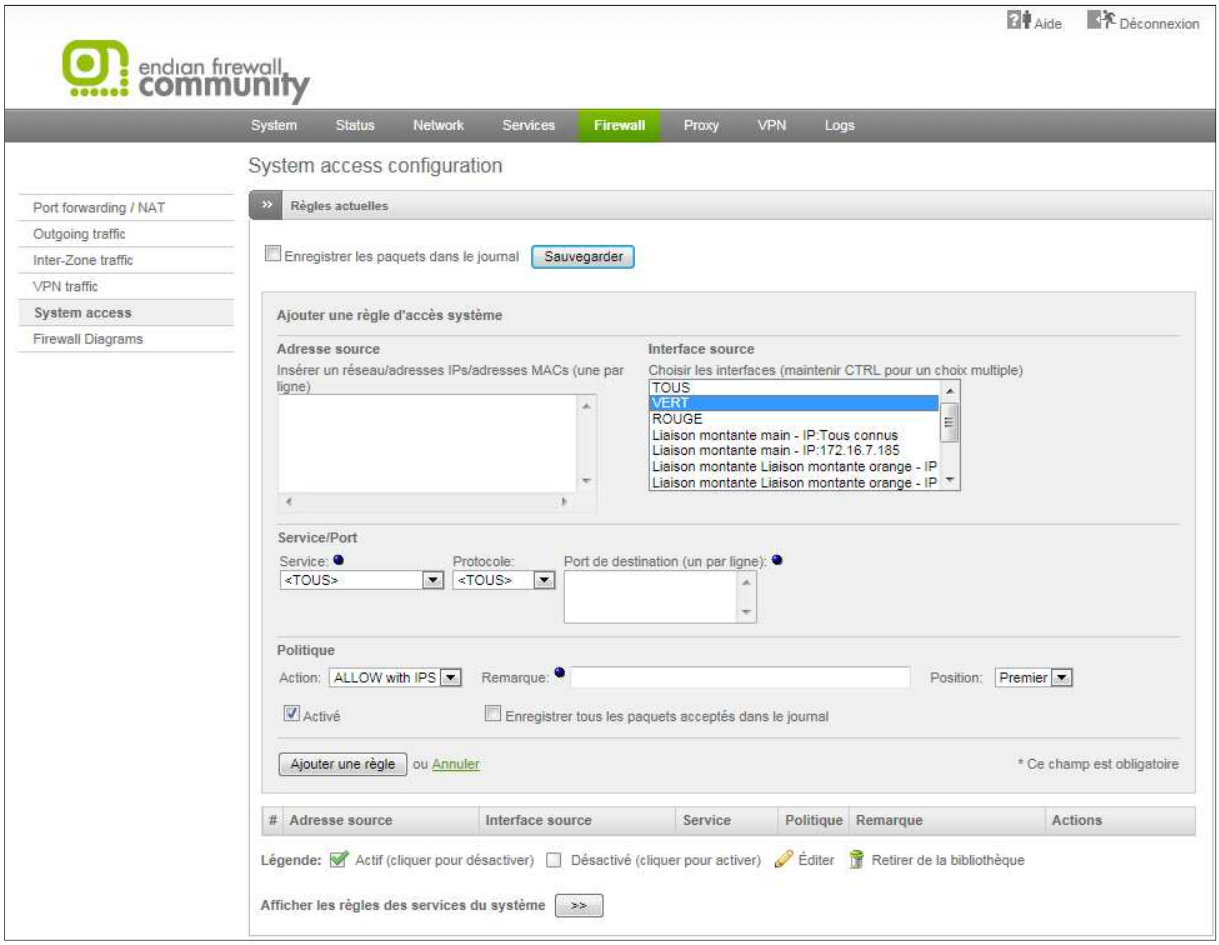
Le firewall VPN permet d'ajouter des règles appliquées aux hôtes qui sont connectés via un VPN.

Par défaut, le firewall VPN est désactivé, ce qui signifie que le trafic entre les hôtes VPN et les hôtes de la zone verte puissent circuler librement, ainsi qu'avec toute les autres zones.

NB :

- Noter que les hôtes VPN ne sont pas soumis aux autres sections du firewall « Inter-Zone traffic » et « Outgoing traffic ».
- La manipulation des règles est identique à la section « Outgoing traffic ».

e) System Access :



Dans cette section, vous pouvez définir des règles qui accordent ou refusent l'accès au firewall Endian lui-même.

f) Firewall Diagrams :

Sur cette page vous pouvez trouver une liste de tous les modules du firewall. Pour chacun des modules, un diagramme a été créé pour mieux comprendre le trafic.

3.6. LE MENU « PROXY » :

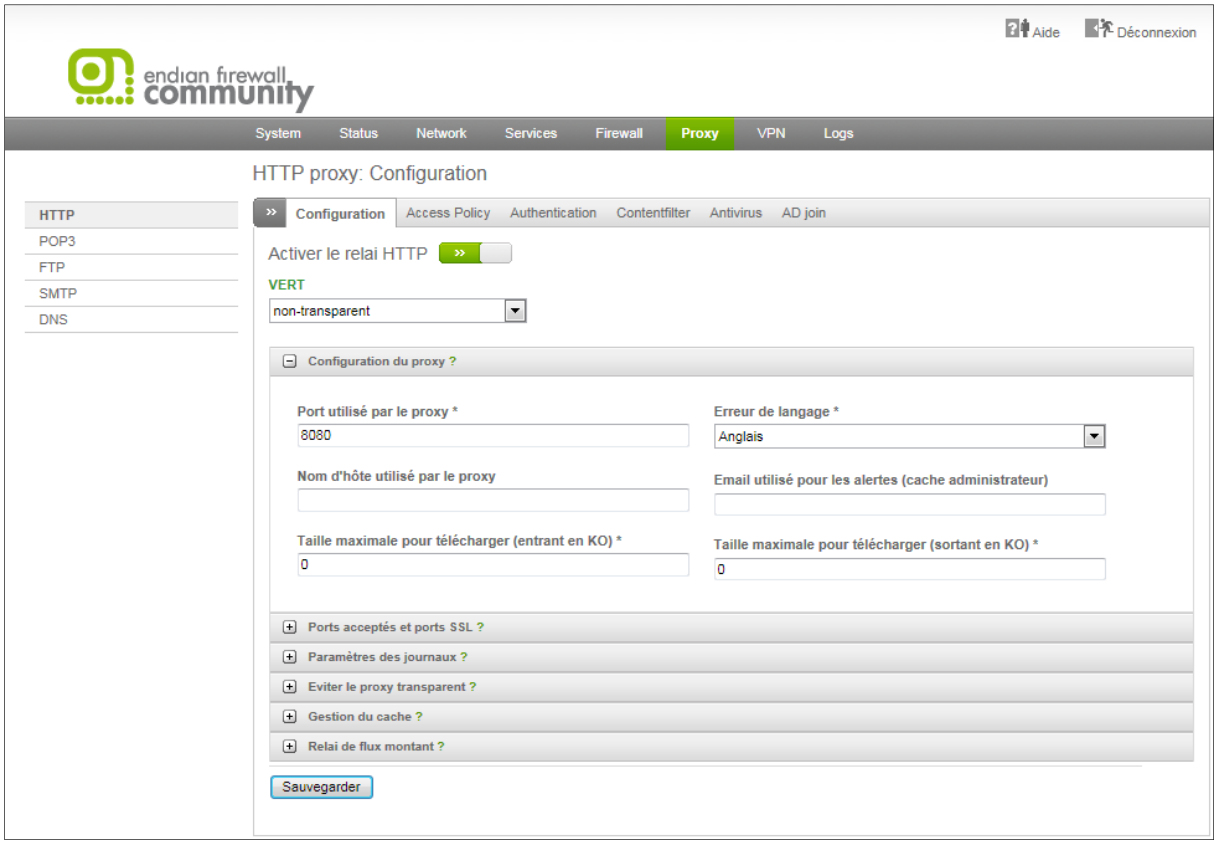
Un proxy est un service sur votre Endian qui peut agir comme un contrôleur d'accès entre les clients et les services réseau.

Si tout le trafic web passe par un proxy on l'appelle proxy transparent. Un proxy non transparent est relié par la configuration de votre navigateur. Voici une liste de proxy qui est disponible sur Endian Firewall. Chaque proxy peut être configuré via les liens qui se trouvent dans le sous-menu sur la côté gauche de l'écran:

- HTTP : configurer le proxy Web, y compris les politiques d'accès, d'authentification, filtrage de contenu et antivirus.
- POP3 : configurer le proxy pour la récupération du courrier via le protocole POP, y compris filtre anti-spam et antivirus.
- FTP : activer ou désactiver le proxy FTP (scan des fichiers, qui sont téléchargés via FTP, pour les virus).

- SMTP : configurer le proxy pour l'envoi ou la récupération du courrier via le protocole SMTP, y compris filtre anti-spam et antivirus.
- DNS : configurer un cache pour le serveur de noms de domaine (DNS), y compris anti-spyware.

HTTP :



Configuration :

- Activez le proxy sur la zone que vous voulez que le trafic http passe à travers lui.(la zone verte, orange ou bleue).
- Choisissez le mode de proxy, soit:

  - Mode transparent : tout le trafic passe à travers lui sans aucune configuration sur les navigateurs.
  - Mode non transparent : vous devez configurer les navigateurs manuellement.

- Configurer les autres champs.

Authentification :

- Endian supporte quatre types d'authentification: Local Authentication (NCSA), LDAP (v2, v3, Novell eDirectory, AD), Windows Active Directory (NTLM) and Radius.
- Chaque type d'authentification nécessite une configuration des paramètres différents.

Access Policy:

- Les politiques d'accès seront appliquées pour tous les clients connectés via le proxy, indépendamment de leur authentification. Les règles de politique d'accès sont les politiques d'accès basé sur : le temps d'accès, la source, la destination, l'authentification, le type de navigateur, les types MIME, détection de virus et filtrage de contenu.
- Vous pouvez sélectionner un type de filtre pour chaque règle pour spécifier si l'accès à internet est bloqué ou autorisé, dans ce dernier cas, vous pouvez activer et sélectionnez un type de filtre.
- Pour ajouter une nouvelle règle suffit de cliquer sur Créer une règle et de remplir vos paramètres.

Content filter :

Pour être en mesure d'utiliser le filtre de contenu, vous devez créer un profil « ContentFilter » dans une règle de politique d'accès. Le filtre de contenu d'Endian (DansGuardian) utilise trois techniques de filtrage qui peuvent être définies chacun par un profil de filtre :

1- Le premier est appelé PICS (Platform for Internet Content Selection). Il est une spécification créée par W3C qui utilise les métadonnées pour les pages Web afin d'aider l'étiquette de contrôle parental.
2- Le second est basé sur un système de pondération de phrase, il analyse le texte des pages web et de calcule un score pour chaque page.
3- La dernière méthode utilise une liste noire d'URL et des domaines. Toutes les URL demandées seront recherchées dans cette liste et ne sont desservies que si elles ne sont pas trouvées.

Antivirus :

Dans cette section vous pouvez configurer le moteur de scanner de virus utilisé par le proxy HTTP. (ClamAV, de Sophos Antivirus est disponible depuis la version 2.3).

- Spécifiez la taille maximale des fichiers qui doivent être scannés par l'antivirus.
- Vous pouvez ajouter une liste d'URL qui ne seront pas scannés par l'antivirus.

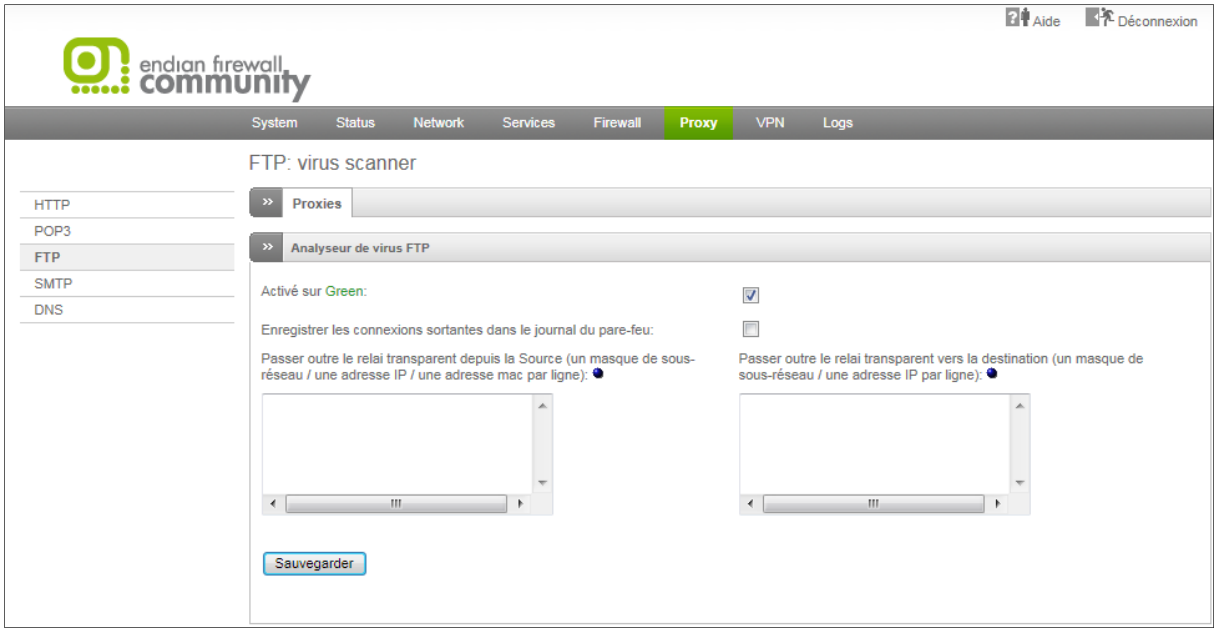
AD join :

Dans cette section, vous pouvez joindre l'annuaire Active Directory. Cela n'est possible que lorsque l'authentification est définie bien sûre sur Windows Active Directory (NTLM).

POP3 :

Dans cette section, vous pouvez activer ou désactiver le proxy POP3 pour chaque zone. Vous pouvez configurer les paramètres globaux du proxy POP3. Il est également possible d'activer l'antivirus et le filtre anti-spam pour les e-mails entrants. Si vous voulez logger chaque connexion sortante POP3, vous pouvez activer « Enregistrer les connexions sortantes dans le journal du pare-feu ».

FTP :



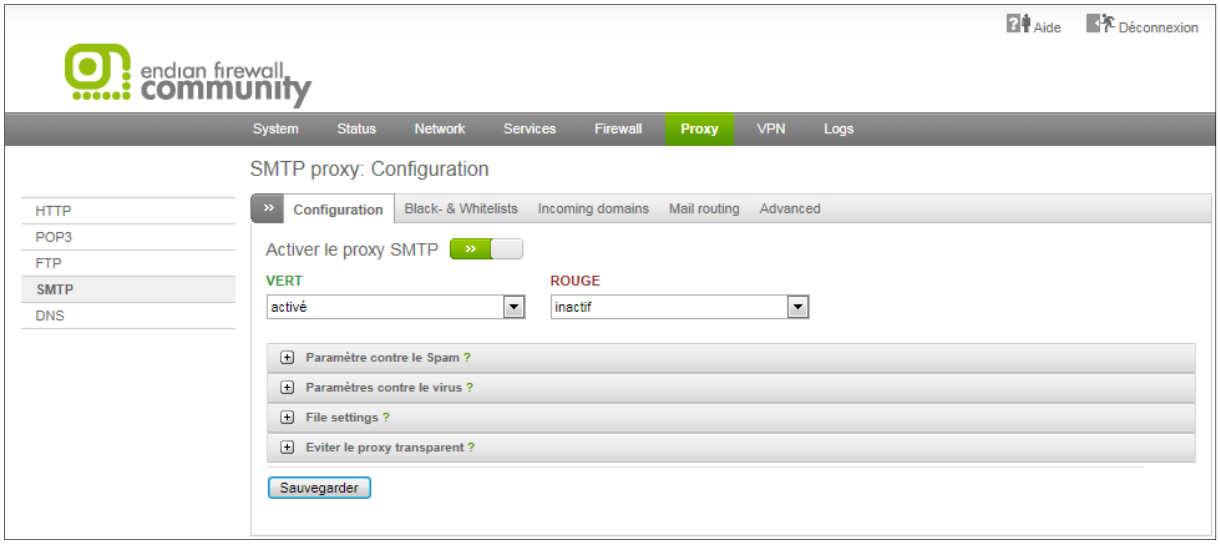
Le FTP (File Transfer Protocol) proxy est disponible seulement comme proxy transparent, ce qui permet la recherche de virus sur les téléchargements FTP.

Vous pouvez activer le proxy transparent FTP sur la zone verte. Les options suivantes peuvent être configurées :

- Enregistrer les connexions sortantes dans le journal du pare-feu.
- Spécifiez les sources (à gauche) ou destinations (à droite), qui ne sont pas soumis à FTP proxy transparent. Toujours spécifier un masque de sous-réseau, une adresse IP ou une adresse mac par ligne par ligne.

    - Passer outre le relai transparent depuis la Source
    - Passer outre le relai transparent vers la destination

SMTP:



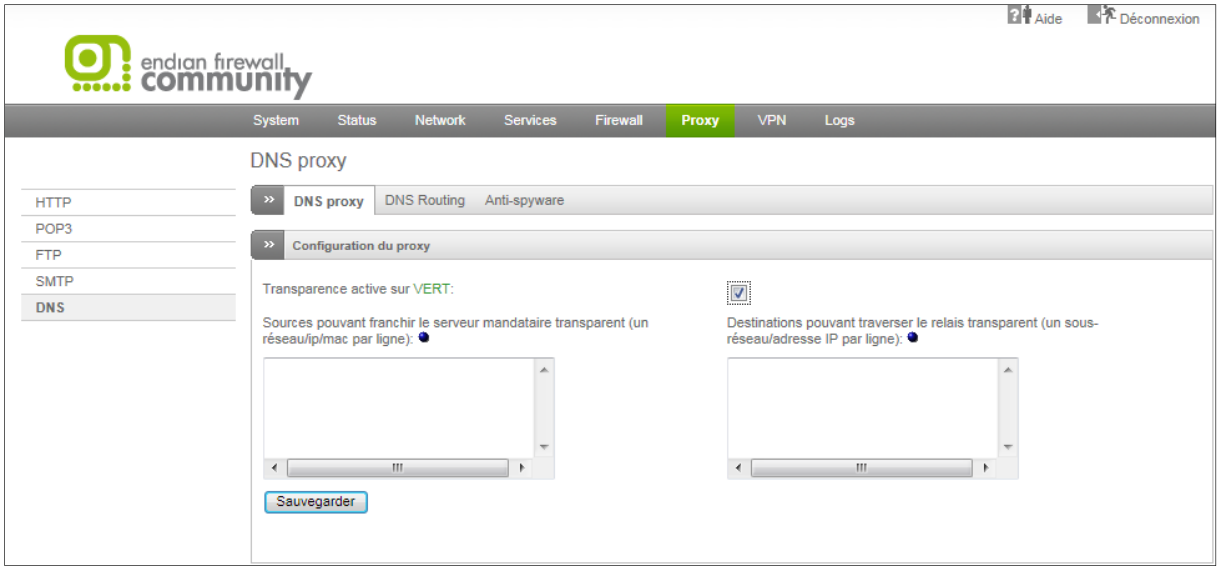
Le proxy SMTP (Simple Mail Transfer Protocol) relais et filtre le trafic e-mail comme il est envoyé vers les serveurs de messagerie.

Le rôle du proxy SMTP est de contrôler et optimiser le trafic SMTP en général et pour protéger votre réseau contre les menaces en utilisant ce protocole.

Le SMTP est utilisé chaque fois qu'un courrier électronique sera envoyé par votre client de messagerie à un serveur à distance (courrier sortant).

Il sera également utilisé si vous avez un serveur de messagerie en cours d'exécution sur votre réseau local (interface VERTE) ou votre DMZ (interface ORANGE) et permettent aux mails envoyés de l'extérieur de votre réseau (demandes entrantes). La configuration de proxy SMTP est divisée en plusieurs sous-sections.

DNS :



Dans cette section, vous pouvez activer le DNS proxy transparent pour la zone verte, orange et zone bleue (si elle est active).

Vous pouvez également définir quels adresses qui ne seront pas soumis à DNS proxy.

- Dans la partie gauche, « Sources pouvant franchir le serveur mandataire transparent », soit un réseau, adresse IP ou adresse mac par ligne.
- Dans la partie droite, « Destinations pouvant traverser le relais transparent », soit un sous-réseau ou adresse IP par ligne.