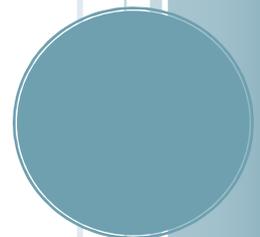


# GUIDE D'INSTALLATION DE FIREWALL OPEN SOURCE

## *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.





**الوكالة الوطنية للسلامة المعلوماتية**  
**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

<b>Présentation d'Endian</b> .....	3
1. Fonctionnement .....	3
2. Installation .....	4
3. Configuration des différents services d'Endian firewall : .....	15
3.1. Le menu « system » : .....	15
3.2. Le menu « status » : .....	15
3.3. Le menu « réseau » : .....	16
3.4. LE MENU « SERVICES » : .....	21
3.5. LE MENU « FIREWALL » : .....	29
3.6. LE MENU « PROXY » : .....	36

# 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 gérés à travers une interface web ( Unified Threat Management UTM).

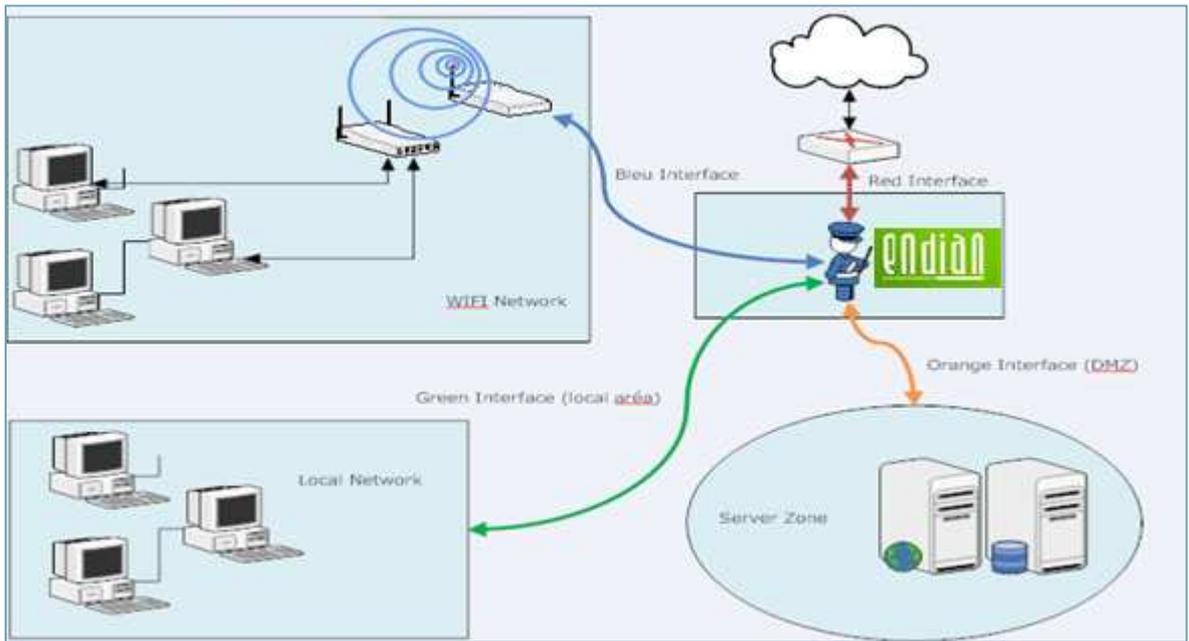
Dans ce guide nous aborderons le fonctionnement des interfaces, l'installation et la configuration d'EFW. Ensuite, nous détaillerons les différents services proposés par Endian.

## 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

```
ISOLINUX 3.31 2006-09-25 Copyright (C) 1994-2005 H. Peter Anvin

Welcome to Endian Firewall, Licensed under GNU GPL version 2.

PLEASE BEWARE! This installation process will kill all
existing partitions on your PC or server. Please be aware
of this before continuing this installation.

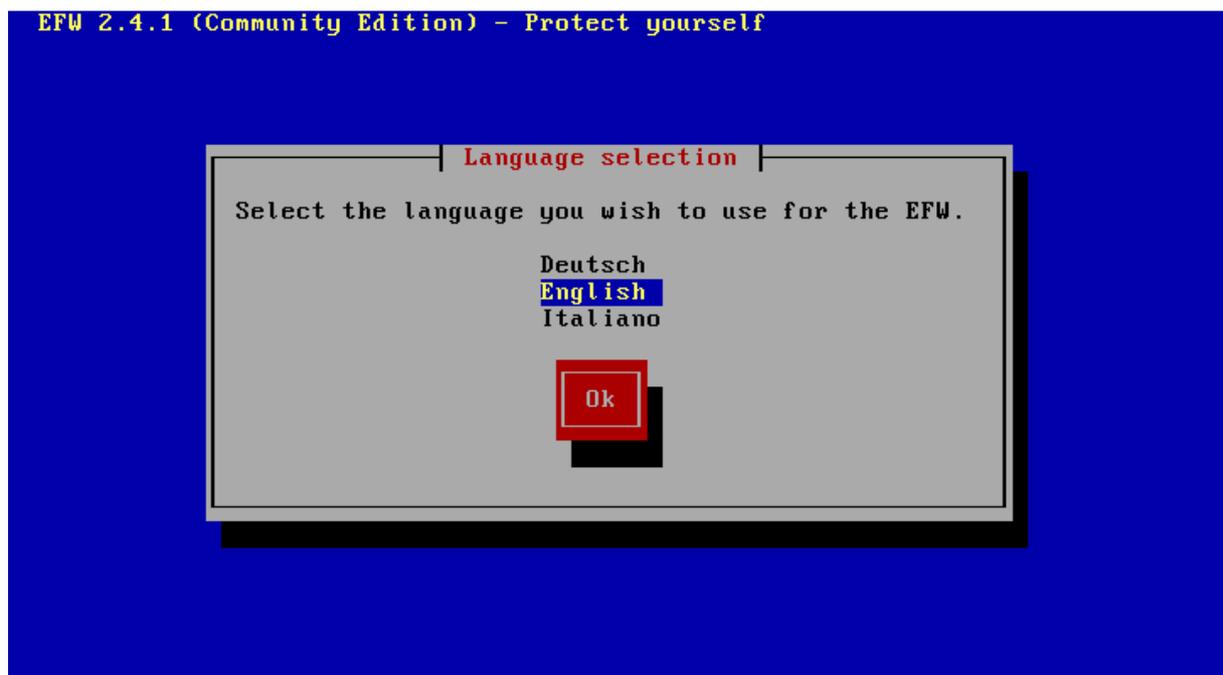
-----
----
---- ALL YOUR EXISTING DATA WILL BE DESTROYED ----
----
-----

Press RETURN to boot Endian Firewall default installation.

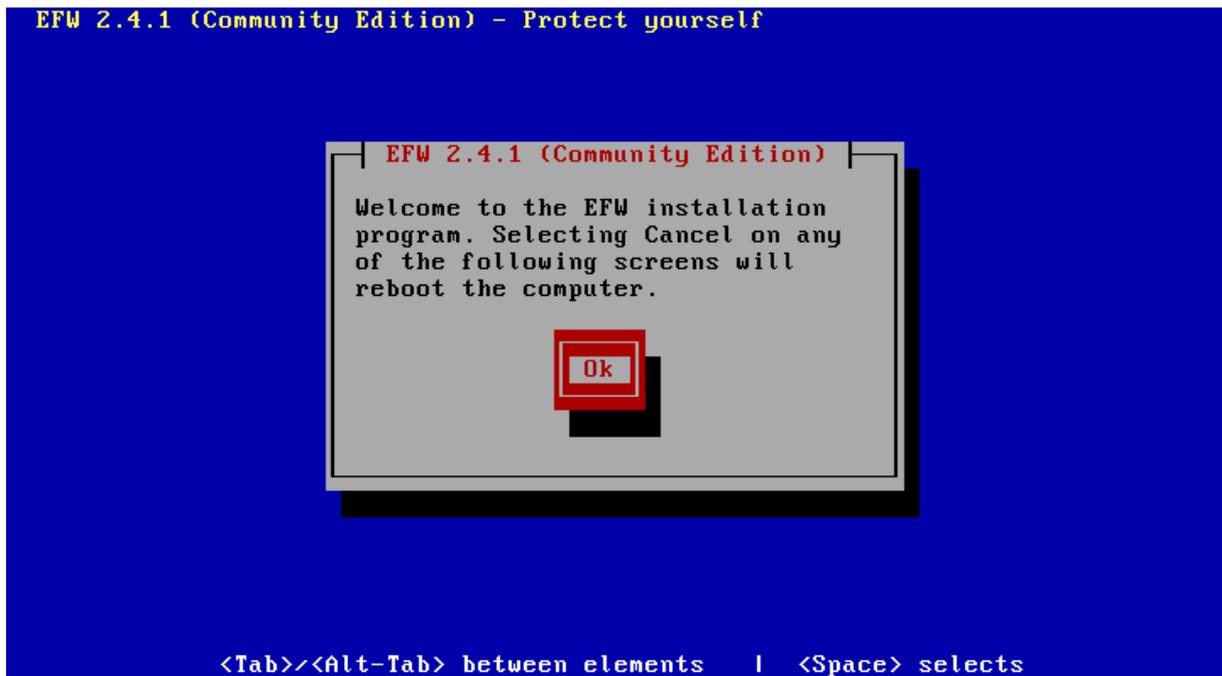
Or, if you are having trouble you can try these options....
Type:  nopcmcia to disable PCMCIA detection
       nousb to disable USB detection
       nousborpcmcia to disable both PCMCIA & USB detection
       dma to enable ide dma (SiS chipset workaround)

boot: _
```

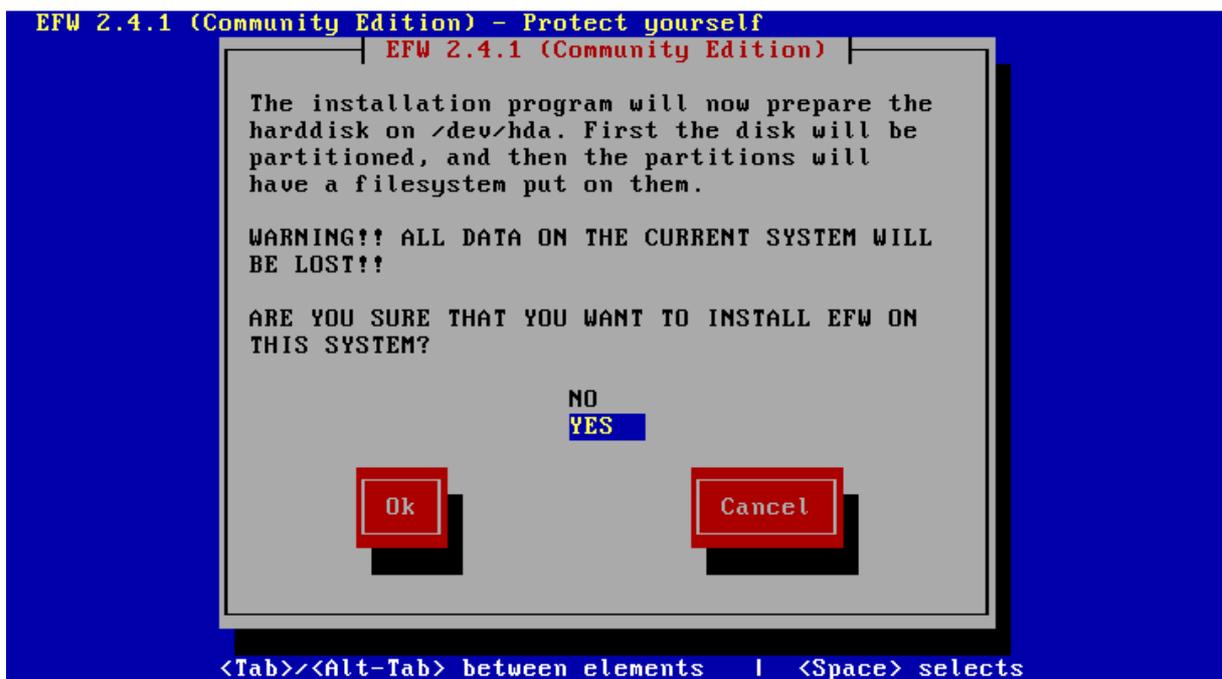
- Tapez sue entrée pour procéder à l'installation



- Choisissez la langue

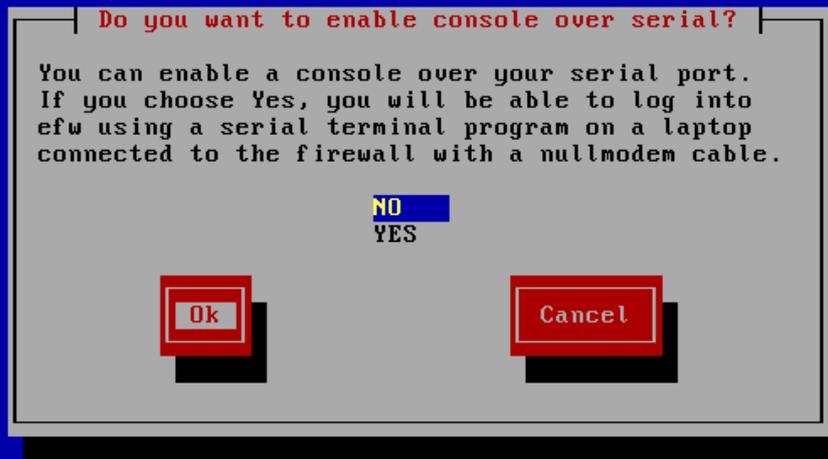


- Cliquez sur « Ok »



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

EFW 2.4.1 (Community Edition) - Protect yourself



<Tab>/<Alt-Tab> between elements | <Space> selects

-

EFW 2.4.1 (Community Edition) - Protect yourself



<Tab>/<Alt-Tab> between elements | <Space> selects

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

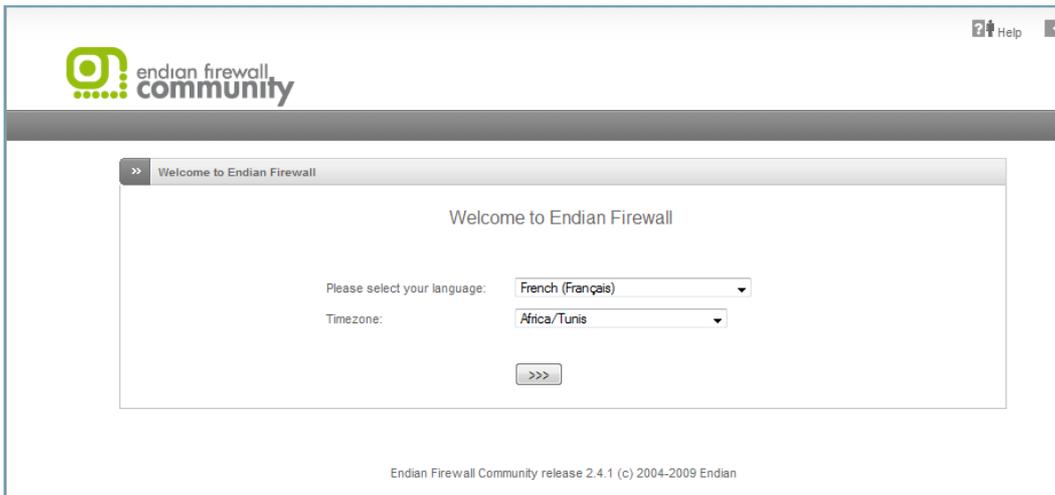
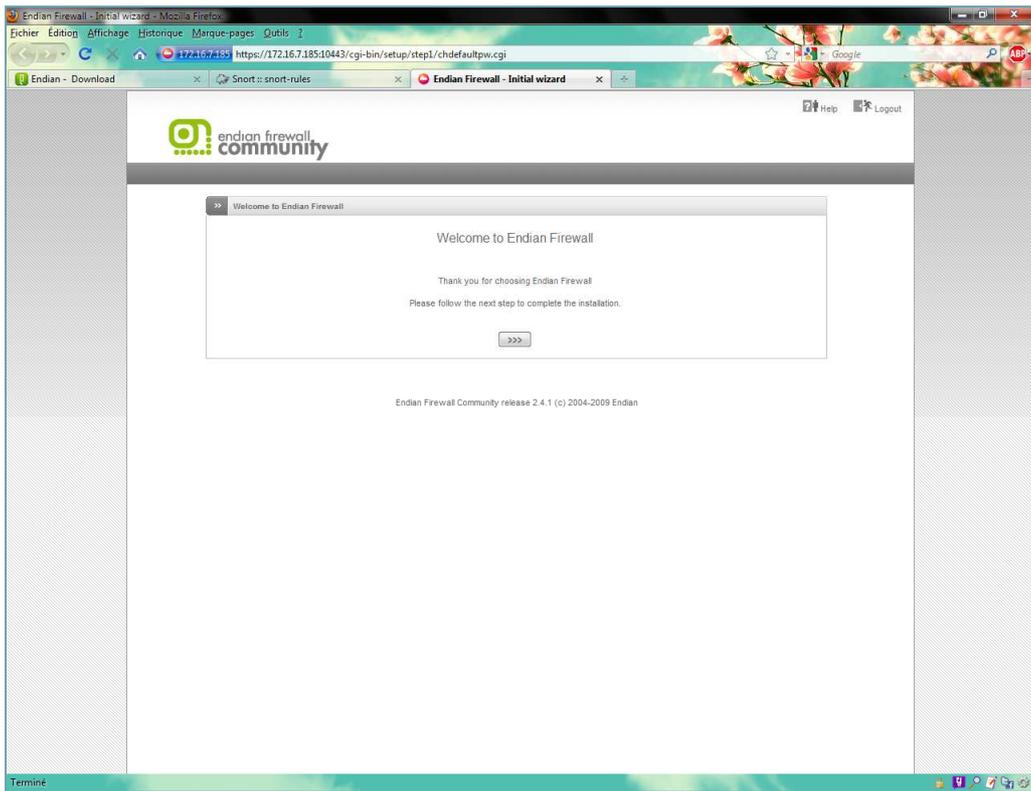
**Congratulations!**

EFW was successfully installed. Please remove any floppy disks or CDRoms in the computer. If your system fails to boot properly, please try booting from a DOS diskette and running 'FDISK /MBR' to re-create the Master Boot Record. Setup will now run where you may configure ISDN, network cards, and the system passwords. After Setup has been completed, you should point your web browser at <http://efw-community> or <https://efw-community:10443> (or whatever you name your EFW), and configure dialup networking (if required) and remote access. Remember to set a password for the EFW 'dial' user, if you wish non EFW 'admin' users to be able to control the link.

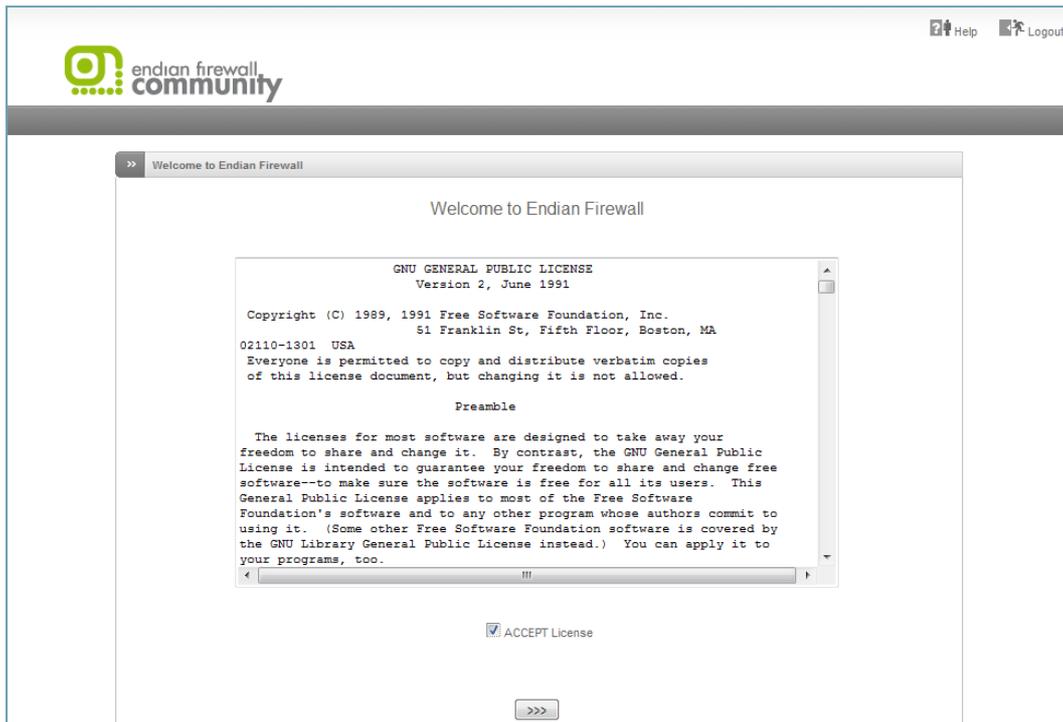


<Tab>/<Alt-Tab> between elements | <Space> selects

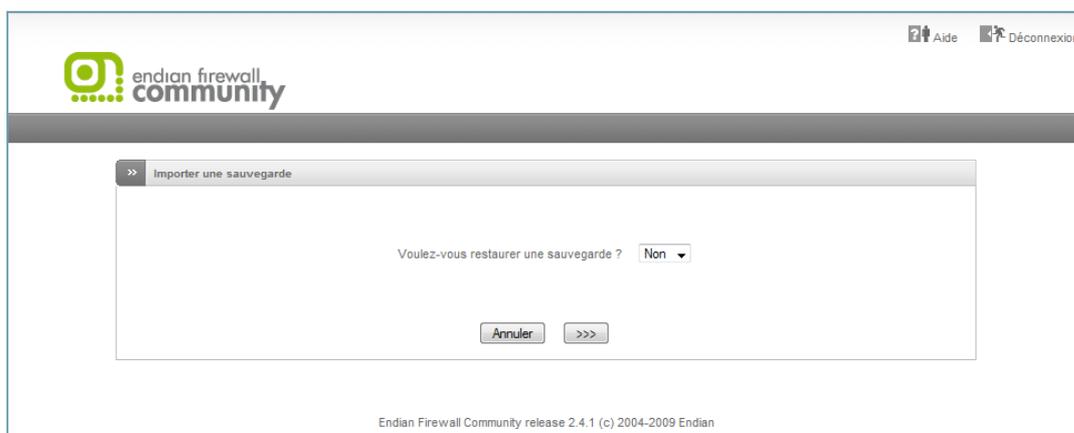
- L'installation d'EFW est termin  cliquez sur « Ok ».
- Une fois l'installation d'Endian Firewall termin  il reste encore   finaliser l'installation via l'interface web. Pour cela lancez un navigateur web et tapez :
  - <http://<l'@IPd'endian>>
  - [https:// <l'@IPd'endian:10443>](https://<l'@IPd'endian:10443>)
- Vous allez  tre redirig  vers l'interface suivante:



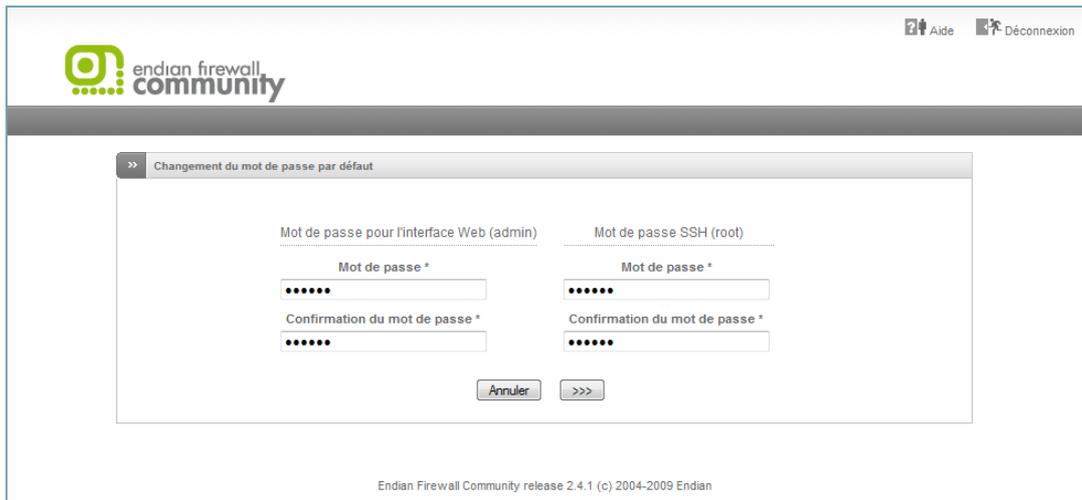
- Choisissez la langue



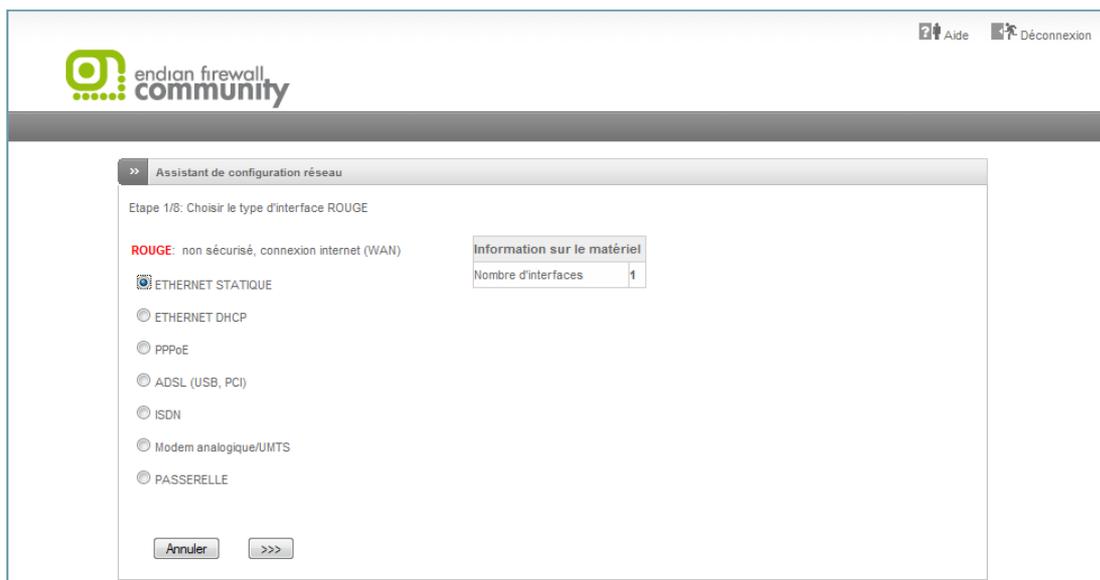
- Faites accepter la License



- Cette option est utile en cas où 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.



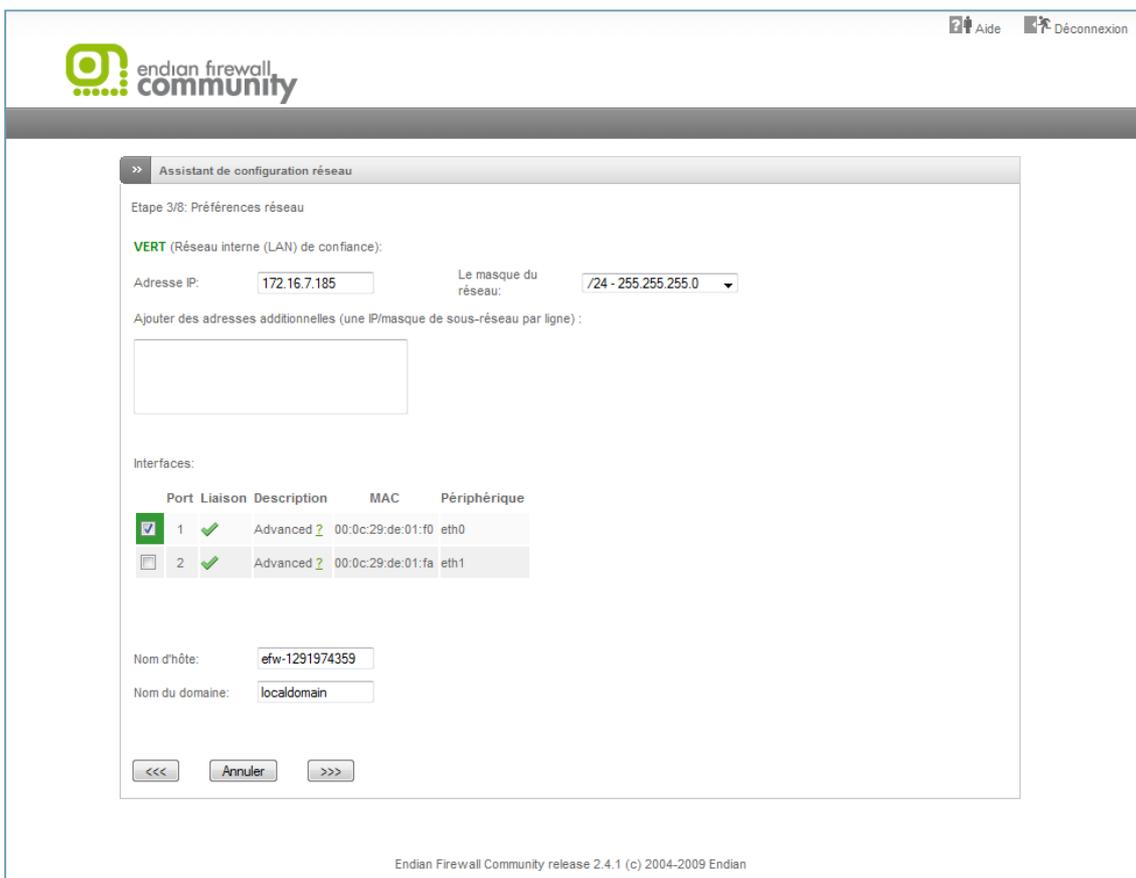
- Choisissez les mots de passe du compte « admin » pour l'interface web et du compte « root » pour se connecter en mode terminal sur le système.



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



- Si vous allez définir 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.

? Aide    Déconnexion

**endian firewall community**

---

**Assistant de configuration réseau**

Etape 4/8: Préférences d'accès à Internet

**ROUGE** (non sécurisé, connexion internet (WAN)):

Adresse IP:       Le masque du réseau:

Ajouter des adresses additionnelles (une IP/masque de sous-réseau par ligne):

Interfaces:

Port	Liaison	Description	MAC	Périphérique
<input type="checkbox"/>	1	✓ Advanced 2	00:0c:29:de:01:f0	eth0
<input checked="" type="checkbox"/>	2	✓ Advanced 2	00:0c:29:de:01:fa	eth1

Passerelle par défaut:

MTU:

Changement de l'adresse MAC avec:

Ce champs peut être laissé vide.

<<<    Annuler    >>>

Endian Firewall Community release 2.4.1 (c) 2004-2009 Endian

- Configurez votre DNS

? Aide    Déconnexion

**endian firewall community**

---

**Assistant de configuration réseau**

Etape 5/8: Configurer la résolution DNS

La configuration manuelle du DNS:

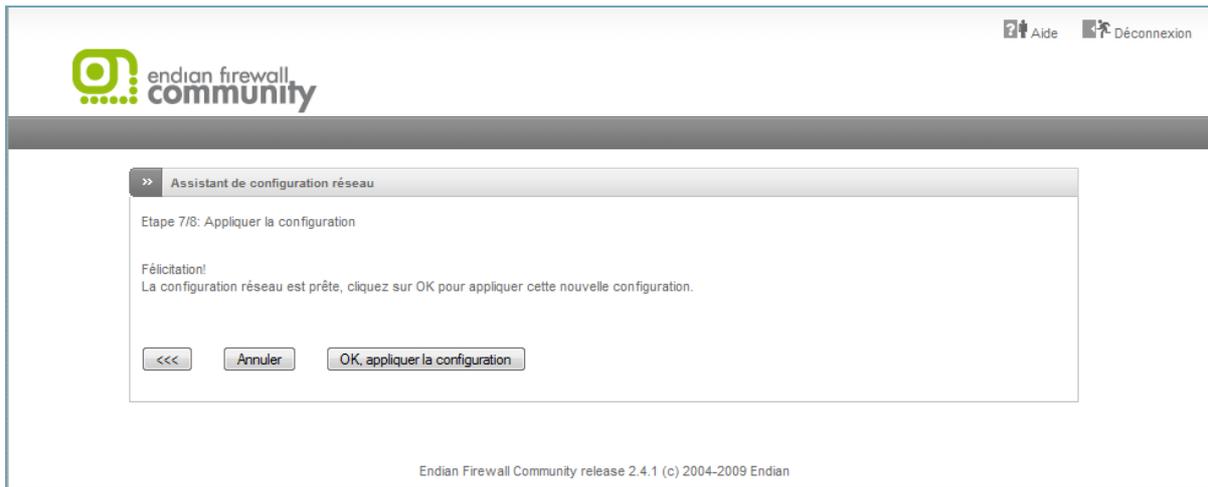
DNS 1:

DNS 2:

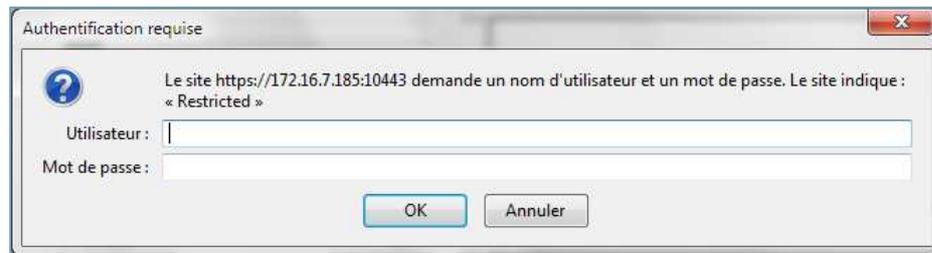
<<<    Annuler    >>>

Endian Firewall Community release 2.4.1 (c) 2004-2009 Endian

- 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.



The screenshot displays the Endian Firewall Community dashboard. At the top, there is a navigation bar with tabs for System, Status, Network, Services, Firewall, Proxy, VPN, and Logs. The main content area is divided into several sections:

- Dashboard:** Shows system information for 'efw-1300096398.localdomain', including hardware (Appareil: Community, Version: 2.4.1, Noyau: 2.6.32.25-57.e40.i586), uptime (16h 1m), and last update (21:19:14).
- Information sur le matériel:** Displays resource usage with progress bars: CPU 1 (47%), Mémoire (58%, 248 MB), disque principal (71%, 564 MB), les données du disque (5%, 839 MB), /var/efw (6%, 99 MB), and /var/log (7%, 418 MB).
- Services (Live log):** Lists services like 'Serveur proxy HTTP' (ON), 'Relai SMTP' (ON), 'POP3 Proxy' (OFF), and 'Détection d'intrusion' (ON). It also shows statistics for proxy hits and SMTP mail status.
- Interfaces réseau:** A table showing network interfaces:
 

Périphérique	Type	Liaison	État	entrant	Sortie
<input checked="" type="checkbox"/> br0	ethernet	Vers le haut	Vers le haut	5.6 KB/s	5.0 KB/s
<input type="checkbox"/> eth0	ethernet	Vers le haut	Vers le haut	5.8 KB/s	5.0 KB/s
<input checked="" type="checkbox"/> eth1	ethernet	Vers le haut	Vers le haut	0.0 KB/s	0.0 KB/s
- Liaisons montantes:** A table showing active connections:
 

Nom	Adresse IP	État	Actif	Géré
Liaison montante principale	172.16.7.185	UP	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
uplink1	123.123.123.123	UP	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

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.

The screenshot shows the 'Services' status page in the Endian Firewall Community interface. The page title is 'System status information' and it includes a navigation menu with 'System', 'Status', 'Network', 'Services', 'Firewall', 'Proxy', 'VPN', and 'Logs'. The 'Status' menu is active. On the left, there is a sidebar with 'System status' selected. The main content area shows a table of services and their status:

Service	Status
Analyseur de virus FTP	STOPPÉ
Antivirus HTTP (havp)	DÉMARRÉ
Filtre du contenu	STOPPÉ
Filtre spam Pyzor	DÉMARRÉ
Filtre spam pour POP3 (spamd)	STOPPÉ
Filtre spam pour SMTP (amavis)	STOPPÉ
Proxy web	DÉMARRÉ
RPV (IPsec)	STOPPÉ
Scanner anti-virus	DÉMARRÉ
Scanner courriel (POP3)	STOPPÉ
Serveur CRON	DÉMARRÉ
Serveur DHCP	STOPPÉ
Serveur NTP	DÉMARRÉ
Serveur OpenVPN	STOPPÉ
Serveur Secure Shell	STOPPÉ
Serveur de journalisation	DÉMARRÉ
Serveur de relai DNS	DÉMARRÉ
Serveur web	DÉMARRÉ
Système de Détection d'Intrusion	DÉMARRÉ

### 3.3. Le menu « réseau » :

The screenshot shows the 'Réseau' (Network) configuration page in the Endian Firewall Community interface. The page title is 'Configuration de l'hôte' and it includes a navigation menu with 'Système', 'État', 'Réseau', 'Services', 'Pare-feu', 'Serveur mandataire (relai)', 'RPV', and 'Journaux'. The 'Réseau' menu is active. On the left, there is a sidebar with 'Edition des hôtes' selected. The main content area shows a table for adding hosts:

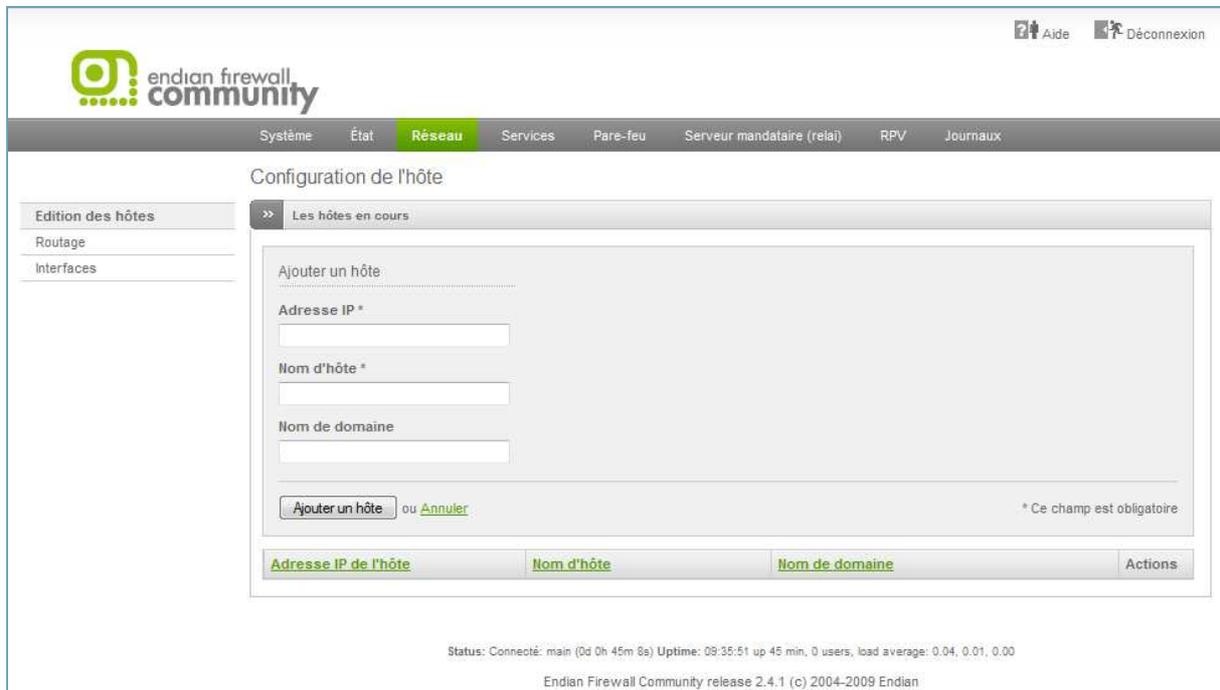
Adresse IP de l'hôte	Nom d'hôte	Nom de domaine	Actions
<a href="#">Ajouter un hôte</a>			

At the bottom of the page, there is a status bar: 'Status: Connecté: main (0d 0h 45m 8s) Uptime: 09:35:51 up 45 min, 0 users, load average: 0.04, 0.01, 0.00' and 'Endian Firewall Community release 2.4.1 (c) 2004-2009 Endian'.

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.

The screenshot displays the Mikrotik WinBox interface for configuring static routing. The top navigation bar includes 'Système', 'État', 'Réseau', 'Services', 'Pare-feu', 'Serveur mandataire (relai)', 'RPV', and 'Journaux'. The 'Réseau' menu is active. The main window is titled 'Éditeur de routage statique' and contains two tabs: 'Routage statique' and 'Règles de routage'. The 'Routage statique' tab is selected, showing a section for 'Ajouter une route'. This section includes the following fields and options:

- Sélecteur:** A dropdown menu.
- Réseau source:** A text input field.
- Réseau de destination:** A text input field.
- Router Via \*:** A dropdown menu set to 'Passerelle statique' and a text input field.
- Activé:** A checked checkbox.
- Remarque:** A text input field.

At the bottom of the form, there are buttons for 'Ajouter la route' and 'Annuler', and a note: '\* Ce champ est obligatoire'.

- Règles de routage :

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

The screenshot shows the Mikrotik WinBox interface for editing routing rules. The main title is 'Éditeur des règles de routage'. The interface is divided into several sections:

- Navigation:** A top menu bar with 'Système', 'État', 'Réseau' (highlighted), 'Services', 'Pare-feu', 'Serveur mandataire (relai)', 'RPV', and 'Journaux'. A left sidebar contains 'Edition des hôtes', 'Routage' (highlighted), and 'Interfaces'.
- Routing Configuration:**
  - 'Routage statique' and 'Règles de routage' tabs are visible.
  - 'Règles actuelles' section shows the current rule configuration.
  - 'Éditeur de règles de politique de routage' section:
    - 'Source \*': Type 'Réseau/IP', with a text area for 'Insérer un réseau/adresses IPs (une par ligne)'.
    - 'Destination \*': Type 'Réseau/IP', with a text area for 'Insérer un réseau/adresses IPs (une par ligne)'.
    - 'Service/Port': 'Service \*' is '<TOUS>', 'Protocole \*' is '<TOUS>', and 'Port de destination (un par ligne)' has an empty text area.
    - 'Router via': 'Liaison montante \*' is 'Liaison montante princip:', with a checkbox 'Utiliser le lien de secours si lien principal tombe'.
    - 'Type de Service': 'non défini', 'Remarque' is an empty text field, and 'Position' is 'Dernier'.
    - Checkboxes: 'Activé' (checked) and 'Enregistrer tous les paquets acceptés dans le journal'.
    - Buttons: 'Créer une Règle' and 'Annuler'.
    - Footnote: '\* Ce champ est obligatoire'.

❖ Interface :

- Éditer 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.

Gestion des liaisons montantes

Édition des hôtes >> Éditer une liaison montante VLANs

Routage >> Liaisons montantes actuelles

Interfaces

Éditer une liaison montante

Description

Type \*

Protocole ADSL \*

modem/routeur ADSL \*

VPI \*  VCI \*

Type d'encapsulation \*

Ajouter d'autres adresses (IP/masque de sous-réseau ou IP/CIDR, une par ligne)

Nom d'utilisateur  Mot de passe

Méthode d'authentification \*

Utiliser des paramètres DNS personnalisés

La liaison montante est activée  Activer la liaison montante au démarrage  La liaison montante est gérée

Si cette liaison montante est indisponible activer

Vérifier si ces hôtes sont disponibles

Paramètres avancés

ou  \* Ce champ est obligatoire

Identifiant	Description	Type	Liaison de secours	Actions
main	Liaison montante principale	Ethernet statique	Aucun	<input checked="" type="checkbox"/> <input type="checkbox"/>

Légende:  Actif (cliquer pour désactiver)  Désactivé (cliquer pour activer)

Status: Connecté: main (0d 8h 22m 24s) Uptime: 17:13:07 up 8:23, 0 users, load average: 0.07, 0.04, 0.00

Endian Firewall Community release 2.4.1 (c) 2004-2009 Endian

- 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.

The screenshot displays the 'Gestionnaire VLAN' (VLAN Manager) interface. At the top, there is a navigation bar with 'Réseau' selected. A sidebar on the left shows 'Interfaces' as the active menu item. The main area is titled 'Ajout d'un nouveau VLAN' (Add a new VLAN) and contains a form with the following fields: 'Interface \*' (dropdown menu showing '1) eth0: Advanced [Etat OK]'), 'Identification du VLAN \*' (text input), and 'Zone \*' (dropdown menu showing 'AUCUN'). There are 'Ajouter VLAN' and 'Annuler' buttons. A note indicates '\* Ce champ est obligatoire' (This field is mandatory). Below the form is a table with the following structure:

Périphérique	Identification du VLAN	sur l'interface	Zone	Actions

At the bottom, the status bar shows: 'Status: Connecté: main (0d 8h 28m 30s) Uptime: 17:19:13 up 8:29, 0 users, load average: 0.00, 0.01, 0.00' and 'Endian Firewall Community release 2.4.1 (c) 2004-2009 Endian'.

### 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.

The screenshot shows the 'Configuration DHCP' page in the Endian Firewall Community web interface. The interface includes a top navigation bar with 'Système', 'État', 'Réseau', 'Services', 'Pare-feu', 'Serveur mandataire (relai)', 'RPV', and 'Journaux'. A sidebar on the left lists various services like 'Serveur DHCP', 'DNS Dynamique', 'Moteur de l'antivirus', etc. The main content area is titled 'Configuration DHCP' and shows settings for 'Interface verte', which is currently 'Activé'. A 'Sauvegarder' button is visible. Below the activation status, there is a 'Paramètres' section with various input fields: 'Adresse de départ' (172.16.7.186), 'Adresse de fin' (172.16.7.254), 'Allow only fixed leases' (checkbox), 'Durée du bail par défaut (min) \*' (60), 'Durée maximum du bail (min) \*' (120), 'Suffixe du nom de domaine' (localdomain), 'Passerelle par défaut \*' (172.16.7.185), 'DNS Primaire' (172.16.7.185), 'DNS Secondaire', 'Serveur NTP principal', 'Serveur NTP secondaire', 'Adresse du serveur WINS principal', and 'Adresse du serveur WINS secondaire'. A 'Tout enregistrer' button and a note '\* Ce champs est requis' are also present. At the bottom, there is a section for 'Baux fixes en cours' with a table header including 'Adresse MAC', 'Adresse IP', 'Adresse suivante', 'Nom de fichier', 'Chemin principal', 'Description', and 'Actions'.

## 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.

Aide Déconnexion

**endian firewall community**

System Status Network **Services** Firewall Proxy VPN Logs

### Dynamic DNS client

>> Les hôtes en cours

**Ajouter un hôte**

Service \*  Derrière un relais  Activer les jokers

Nom d'hôte \*  Domaine \*

Nom d'utilisateur \*  Mot de passe \*

Derrière un Routeur (NAT)  Activé

ou [Annuler](#) \* Ce champ est obligatoire

Service	Nom d'hôte	Domaine	Relai web anonyme	Jokers	Activé	Actions
dhs.org	ansi	ansi.tn	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	

Légende:  Actif (cliquer pour désactiver)  Désactivé (cliquer pour activer) Éditer Retirer de la bibliothèque

### 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.

endian firewall community

Aide Déconnexion

System Status Network **Services** Firewall Proxy VPN Logs

### Clamav AntiVirus

>> Clamav AntiVirus

>> Configuration de Clamav

Anti Archivebomb

Taille maximale de l'archive \* Nombre maximal d'archives imbriquées \*

50 5

Max. fichiers dans l'archive \* Ratio de compression maximal \*

1000 1000

Gestion des mauvaises archives \*

Accepter sans vérifier

Interdire les archives chiffrées

Sauvegarder

La mise à jour programmée des signatures Clamav

Toutes les heures ?

Quotidien ?

Hebdomadairement ?

Mensuellement ?

>> Signatures des virus de Clamav

Dernière mise à jour de signatures sur depuis pour un total de signatures.

Dernière vérification de synchronisation	Type	Version	Total	Dernière mise à jour
	Signatures principales			
	Les signatures volatiles			

Mettre à jour les signatures maintenant ou Chercher dans la base de données des virus en ligne

#### 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.

The screenshot shows the Endian Firewall Community web interface. At the top, there is a navigation bar with the following tabs: System, Status, Network, Services (highlighted), Firewall, Proxy, VPN, and Logs. The main content area is titled "Time server" and is divided into two sections:

- Utiliser un serveur de temps**: This section includes a "Paramètres" area with a checked checkbox "Outrepasser les serveur de temps par défaut \*". Below this is a scrollable area for configuration, followed by a "Fuseau horaire \*" dropdown menu set to "Africa/Tunis". At the bottom of this section are two buttons: "Sauvegarder" and "Synchroniser maintenant".
- Réglez manuellement**: This section contains input fields for "Année: 2011", "Mois: 5", "Jour: 25", "Heures: 22", and "Minutes: 36", followed by a "Régler l" button.

### 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.

endian firewall community

Aide Déconnexion

System Status Network **Services** Firewall Proxy VPN Logs

### Spam Training

>> Sources actuelle d'apprentissage de spam

Éditer la configuration par défaut Test des connexions Commencer l'apprentissage maintenant

>> Edition de la configuration

Hôte IMAP par défaut

Nom d'utilisateur par défaut  Mot de passe par défaut

Dossier non-spam par défaut  Dossier de spam par défaut

programmation de l'apprentissage automatique du filtre de spam

Désactivé  Toutes les heures ?  Quotidien ?  Hebdomadairement ?  Mensuellement ?

Sauvegarder

Ajout d'une source d'apprentissage pour le spam IMAP

Hôte IMAP	Nom d'utilisateur	Dossier non-spam	Dossier Spam	Remarque	Connexion	Actions
						<input checked="" type="checkbox"/> Actif (cliquer pour désactiver) <input type="checkbox"/> Désactivé (cliquer pour activer)  Éditer  Retirer de la bibliothèque  Tester la connexion

>> SpamAssassin Rule Update Schedule

Schedule for SpamAssassin rule updates

Toutes les heures ?  Quotidien ?  Hebdomadairement ?  Mensuellement ?

Sauvegarder

#### f) Prévention d'intrusion:

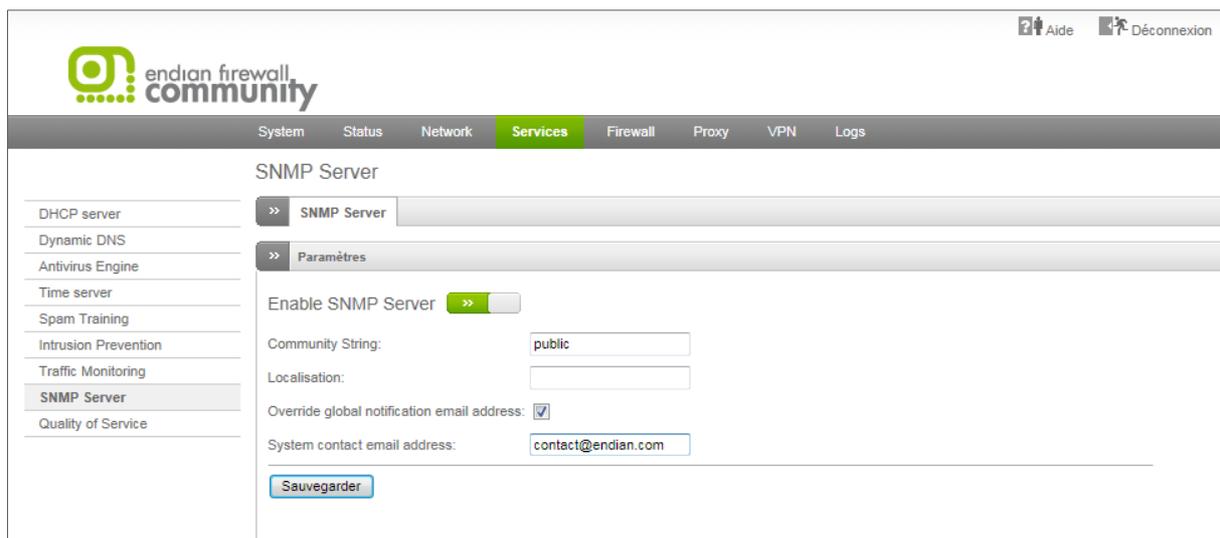
- Endian inclut comme moteur de détection d'intrusion système « snort ».
- Vous pouvez l'activer seulement sur la zone verte.
- Pour les règles de snort, soit :
  - D'activer l'option de récupération des règles automatiquement et de planifier les mises à jour.
  - D'importer des règles personnalisées 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.

Endian Firewall - Quality of Service Devices

» Périphériques Classes Règles

Ajouter le périphérique de qualité de service

Périphérique Cible: Interface 2

Bande passante entrante (Ko/s): 10000

Bande passante sortante (Ko/s): 10000

Enabled:

Add or Annuler \* Ce champ est obligatoire

Périphérique	Bande passante entrante (Ko/s)	Bande passante sortante (Ko/s)	Actions
Interface 1 [VERT]	1000	1000	

### 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 trafic 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:

The screenshot shows the Endian Firewall Community web interface. At the top, there is a navigation menu with 'Firewall' highlighted. Below it, the page title is 'Port forwarding / Destination NAT'. On the left, there is a sidebar with various traffic types. The main content area shows a table for 'Règles actuelles' (Active Rules) with columns for '#', 'Adresse IP entrante', 'Service', 'Politique', 'Translate to', 'Remarque', and 'Actions'. Below the table, there is a legend for rule status (Active/Inactive) and a button to 'Afficher les règles du système'.

### - Destination NAT :

Destination NAT est généralement utilisé pour permettre l'accès réseau limité à partir d'un réseau non sécurisé, ou de traduire 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 propre 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.

The screenshot shows the 'Source Network Address Translation' configuration page in the Endian Firewall community web interface. The page is titled 'Éditeur de règles source NAT' and contains several sections:

- Source:** Type is 'Réseau/IP'. The text area contains '10.10.10.5'.
- Destination:** Type is 'Réseau/IP'. The text area is empty.
- Service/Port:** Service is 'SMTP', Protocole is 'TCP', and Port de destination is '25'.
- NAT:** NAT is selected, and the dropdown for 'vers une adresse source' is set to 'Liaison montante Liaison montante'.
- Activé:** The checkbox is checked.
- Buttons:** 'Éditer la Règle' and 'Annuler' buttons are visible.
- Note:** '\* Ce champ est obligatoire' is displayed at the bottom right.

- 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 firewall community

System Status Network Services **Firewall** Proxy VPN Logs

Outgoing firewall configuration

Port forwarding / NAT  
**Outgoing traffic**  
 Inter-Zone traffic  
 VPN traffic  
 System access  
 Firewall Diagrams

>> Règles actuelles

[Ajouter une nouvelle règle pour le pare-feu](#)

#	Source	Destination	Service	Politique	Remarque	Actions
1	VERT BLEU	ROUGE	TCP/80		allow HTTP	
2	VERT BLEU	ROUGE	TCP/443		allow HTTPS	
3	VERT	ROUGE	TCP/21		allow FTP	
4	VERT	ROUGE	TCP/25		allow SMTP	
5	VERT	ROUGE	TCP/110		allow POP	
6	VERT	ROUGE	TCP/143		allow IMAP	
7	VERT	ROUGE	TCP/995		allow POP3s	
8	VERT	ROUGE	TCP/993		allow IMAPs	
9	VERT ORANGE BLEU	ROUGE	TCP+UDP/53		allow DNS	
10	VERT ORANGE BLEU	ROUGE	ICMP/8 ICMP/30		allow PING	

Légende  Actif (cliquer pour désactiver)  Désactivé (cliquer pour activer) Éditer Retirer de la bibliothèque

Afficher les règles du système >>>

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:

endian firewall community

Aide Déconnexion

System Status Network Services **Firewall** Proxy VPN Logs

### Inter-Zone firewall configuration

>> Règles actuelles

Ajouter une règle de zone au pare-feu

Source  
Type \* Réseau/IP

Destination  
Type \* Zone/Interface

Ajouter le(s) Réseau(x)/IP(s) (un par ligne):

Choisir les interfaces (maintenir CTRL pour un choix multiple):  
VERT  
Interface 1 (Zone: VERT)

Service/Port  
Service \* <TOUS> Protocole \* <TOUS> Port de destination (un par ligne)

Politique  
Action \* ALLOW with IPS Remarque Position \* Dernier

Activé  Enregistrer tous les paquets acceptés dans le journal

Ajouter une règle ou Annuler \* Ce champ est obligatoire

#	Source	Destination	Service	Politique	Remarque	Actions
1	VERT	VERT	<TOUS>	→		↓ ↑ ✓ ✎ 🗑
2	VERT	BLEU	<TOUS>	→		↓ ↑ ✓ ✎ 🗑
3	VERT	ORANGE	<TOUS>	→		↓ ↑ ✓ ✎ 🗑
4	BLEU	BLEU	<TOUS>	→		↓ ↑ ✓ ✎ 🗑
5	ORANGE	ORANGE	<TOUS>	→		↓ ↑ ✓ ✎ 🗑

Légende:  Actif (cliquer pour désactiver)  Désactivé (cliquer pour activer) ✎ Éditer 🗑 Retirer de la bibliothèque

Afficher les règles des services du système >>>

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 activer/désactiver, 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 :

The screenshot shows the 'Éditeur de règle du pare-feu RPV' (VPN Firewall Rule Editor) in the Endian Firewall Community interface. The 'Règles actuelles' (Current Rules) section is active. The rule configuration includes:

- Source:** Type \* Réseau/IP
- Destination:** Type \* Zone/RPV/Liaison montante. A dropdown menu is open showing options: ROUGE, VERT + OPENVPN (selected), IPSEC, Liaison montante main [ROUGE], and Liaison montante orange [ROUGE].
- Service/Port:** Service \* <TOUS>, Protocole \* <TOUS>, Port de destination (un par ligne)
- Politique:** Action \* ALLOW with IPS, Remarque, Position \* Premier
- Activé
- Enregistrer tous les paquets acceptés dans le journal
- Buttons: Créer une règle, Annuler
- Footnote: \* Ce champ est obligatoire

Legend (Légende):

- Actif (cliquer pour désactiver)
- Désactivé (cliquer pour activer)
- Éditer
- Retirer de la bibliothèque

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 toutes 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 :

The screenshot shows the 'System access configuration' page in the Endian Firewall Community web interface. The page is titled 'Règles actuelles' and includes a sidebar with navigation options like 'Port forwarding / NAT', 'Outgoing traffic', 'Inter-Zone traffic', 'VPN traffic', 'System access', and 'Firewall Diagrams'. The main content area is for adding a system access rule, with fields for 'Adresse source', 'Interface source', 'Service/Port', and 'Politique'. The 'Interface source' dropdown is open, showing options like 'TOUS', 'VERT', 'ROUGE', and several 'Liaison montante' options. The 'Action' is set to 'ALLOW with IPS' and the rule is checked as 'Activé'. A legend at the bottom explains the status icons and provides a button to 'Afficher les règles des services du système'.

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

f) Firewall Diagrams :

endian firewall community

System Status Network Services **Firewall** Proxy VPN Logs

Endian Firewall - Firewall Diagrams

- Transfert de port / NAT
- Trafic sortant
- Trafic Inter-Zone
- Trafic VPN
- Accès système
- Diagramme du Pare-Feu

The screenshot displays the 'Endian Firewall - Firewall Diagrams' interface. On the left, a sidebar lists several traffic types: 'Transfert de port / NAT', 'Trafic sortant', 'Trafic Inter-Zone', 'Trafic VPN', 'Accès système', and 'Diagramme du Pare-Feu'. The main content area shows four diagrams arranged in a 2x2 grid. The top-left diagram is titled 'Transfert de port / NAT' and shows traffic from a cloud (Internet) passing through a firewall (labeled 'Firewall') to a laptop. The top-right diagram is titled 'Trafic VPN' and shows traffic from a cloud passing through a firewall to a laptop. The bottom-left diagram is titled 'Trafic sortant' and shows traffic from a laptop passing through a firewall to a cloud. The bottom-right diagram is titled 'Trafic entrant routé' and shows traffic from a cloud passing through a firewall to a laptop. Each diagram includes labels for 'UP1', 'UP2', and 'UP3' ports on the firewall.

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 :](#)

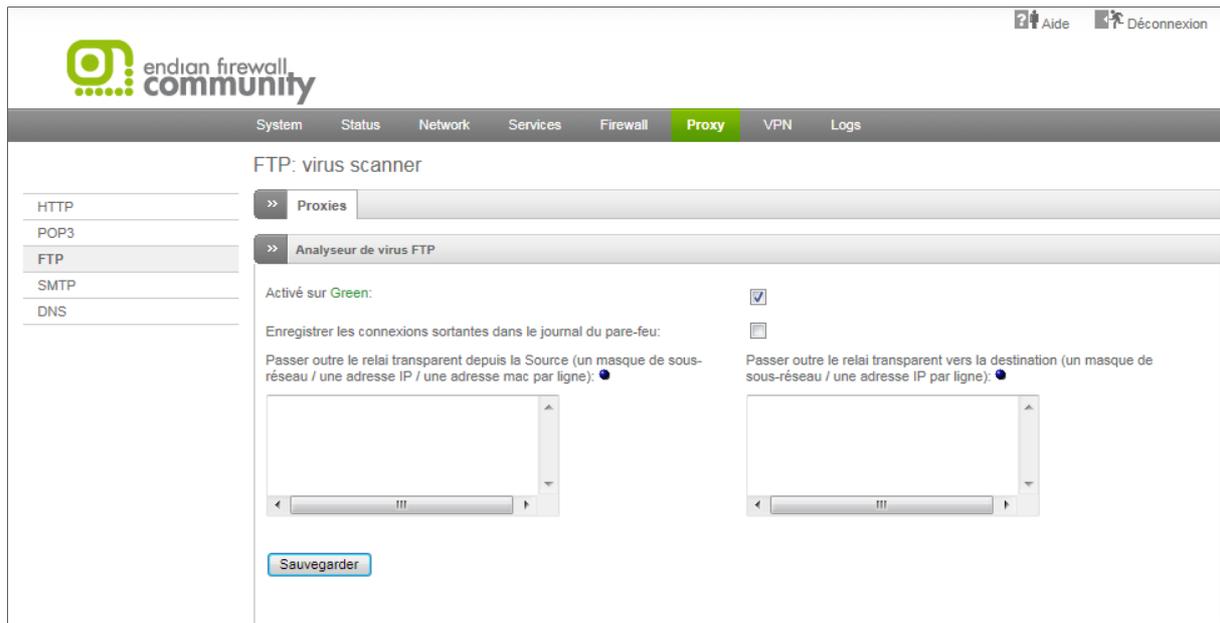
Dans cette section, vous pouvez joindre l'annuaire Active Directory. Cela n'est possible que lorsque l'authentification est définie bien sûre sur Windows Active Directory (NTLM).

## 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 :

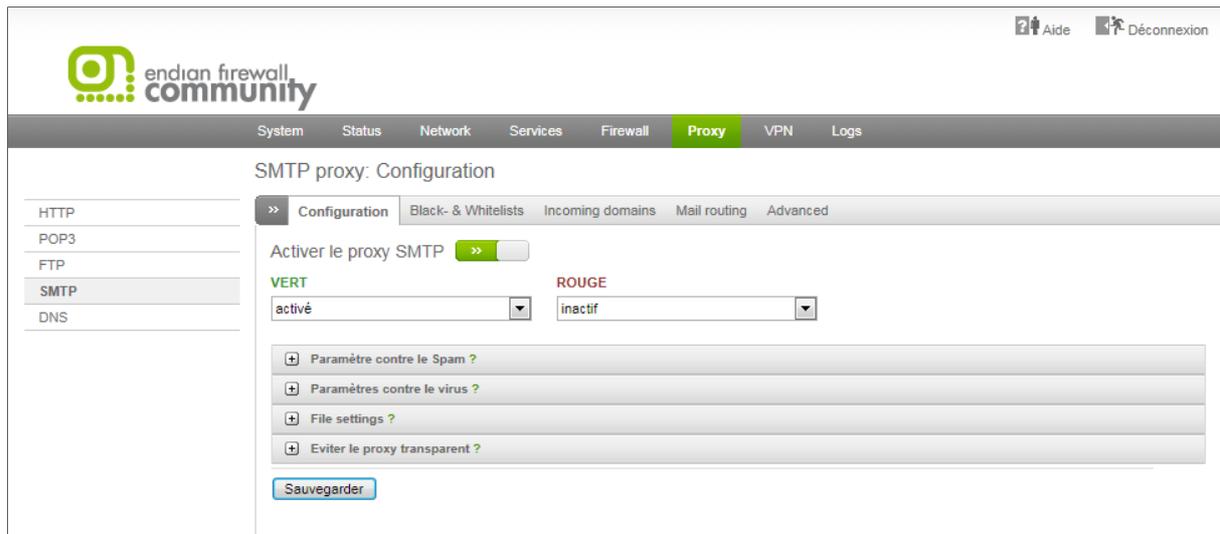


Le FTP (File Transfer Protocol) proxy est disponible seulement comme proxy transparent, ce qui permet la recherche de virus sur les téléchargements FTP.

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:



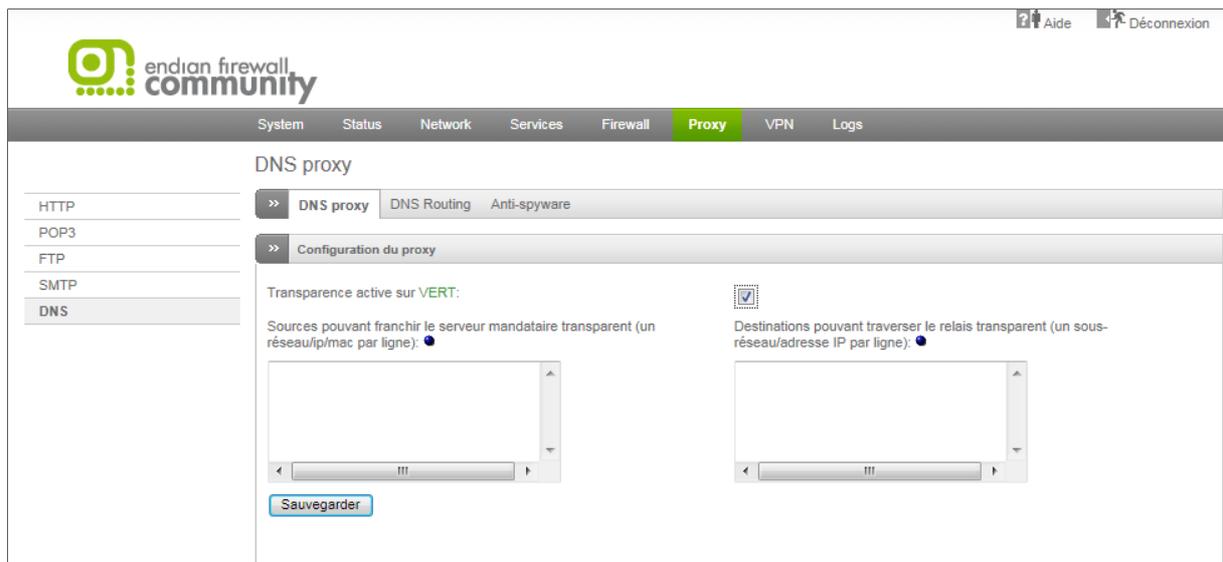
Le proxy SMTP (Simple Mail Transfer Protocol) relaie et filtre le trafic e-mail comme il est envoyé vers les serveurs de messagerie.

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.