D-Link®
Building Networks for People

DFL-1100
GUIDE D'INSTALLATION

Contenu du paquet

- Pare-feu de sécurité réseau D-Link® NETDEFEND™ DFL-1100
- Câble Ethernet Straight-Through CAT5 UTP
- Câble inverseur CAT5 UTP
- Câble RS-232 d'interface vers la console
- CD-ROM (contenant le manuel)
- Cordon d'alimentation

Configuration requise

- Ordinateur comportant une carte Ethernet et un système d'exploitation Windows, Mac ou Unix.
- Internet Explorer ou Netscape Navigator à partir de la version 6.0, avec JavaScript actif.

Présentation du matériel

Panneau avant

Voyant	Signification
Liaison	Un vert continu signifie que la connexion fonctionne sur le port dont le numéro est indiqué.
Fonctionnement	Le voyant « **Fonctionnement** » clignote pendant la transmission des données sur le port dont le numéro est indiqué.
Secteur	Lorsqu'il est allumé en continu, ce voyant signifie que l'équipement est alimenté correctement.
Etat	Ce voyant doit clignoter lorsque l'équipement est en fonctionnement normal. (Si le voyant d'état est allumé en continu, veuillez prendre contact avec le support technique D-Link.)

Port	Description
Console	A raccorder directement au port série de votre ordinateur au moyen du câble RS-232 pour configurer le pare-feu. (Paramètres de la console : Vitesse : 9600 bauds, Nombre de bits de données : 8, Parité : Sans, Nombre de bits de stop : 1)
WAN	A raccorder à votre routeur externe, modem DSL ou modem câble.
LAN	A raccorder à votre réseau interne.
DMZ	A raccorder aux serveurs internes qui doivent être visibles depuis Internet (FTP, SNMP, HTTP et DNS).
ETH4/Sync	En mode haute disponibilité, peut servir de port LAN, de port DMZ ou d'interface Sync supplémentaire.

Panneau arrière

Elément	Description
Connecteur d'alimentation	Emplacement pour brancher le cordon secteur.
Interrupteur Marche/Arrêt	Allume ou éteint l'appareil.
Ventilateur	Veillez à installer l'appareil dans un endroit convenablement ventilé et à ne pas obstruer les orifices de ventilation.

Installation matérielle

1. Branchez le cordon secteur dans le connecteur correspondant situé sur le panneau arrière du DFL-1100. Branchez l'autre extrémité à la prise murale ou à la prise multiple.
2. Actionnez l'interrupteur situé sur le panneau arrière du DFL-1100. Le voyant d'alimentation s'allume.
3. Eteignez votre modem large bande. Certains modems ne sont pas équipés d'un interrupteur marche/arrêt : il vous faut dans ce cas débrancher le cordon secteur.
4. Branchez un câble Ethernet au connecteur correspondant de votre modem large bande. Connectez-en ensuite l'autre extrémité au port WAN situé sur le panneau avant du DFL-1100.
5. Mettez sous tension le modem large bande. Au bout des quelques secondes nécessaires à l'initialisation de votre modem, le voyant correspondant au port WAN doit s'allumer pour indiquer que la connexion est établie.
6. Connectez un câble Ethernet au port LAN situé sur le panneau avant du DFL-1100. Branchez-en l'autre extrémité au hub réseau ou au switch. Le voyant correspondant au port LAN doit s'allumer pour indiquer que la connexion est établie.
7. Connectez au hub réseau ou au switch (si ce n'est pas déjà fait) l'ordinateur que vous allez utiliser pour configurer le DFL-1100. Assurez-vous que le PC de configuration est paramétré de façon à obtenir automatiquement une adresse IP. Il peut s'avérer nécessaire de révoquer puis de renouveler l'adresse IP.

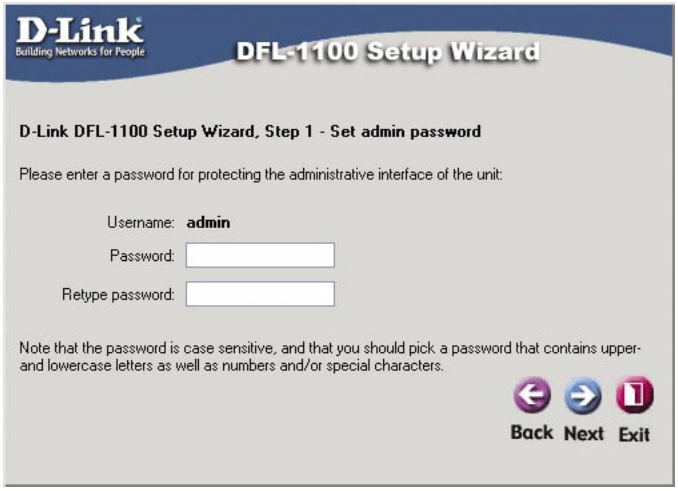
L'assistant d'installation

La configuration du DFL-1100 s'appuie sur une interface web. Vous pouvez configurer votre DFL-1100 à l'aide d'Internet Explorer ou de Netscape Navigator à partir de la version 6.0 avec JavaScript actif. Pour accéder à l'écran de paramétrage, lancez votre navigateur, saisissez l'adresse IP du DFL-1100 dans le champ d'adresse puis tapez sur la touche « Entrée ». Ainsi, si vous utilisez l'adresse par défaut du DFL-1100's, vous devez saisir « **https://192.168.1.1** » *(Remarque: Prenez soin de veiller à la présence du « **s** »" à la fin de « **https** » pour garantir le recours à une connexion sécurisée).*

Une fois que vous vous êtes connecté au DFL-1100, l'assistant d'installation démarre automatiquement. Il est recommandé de se connecter exclusivement à l'aide du protocole HTTP sécurisé. Pour ce faire, sélectionnez « **Secure HTTP (HTTPS) only** » **(HTTP sécurisé (HTTPS) exclusivement)** et cliquez sur « **Next** » **(Suivant)**.

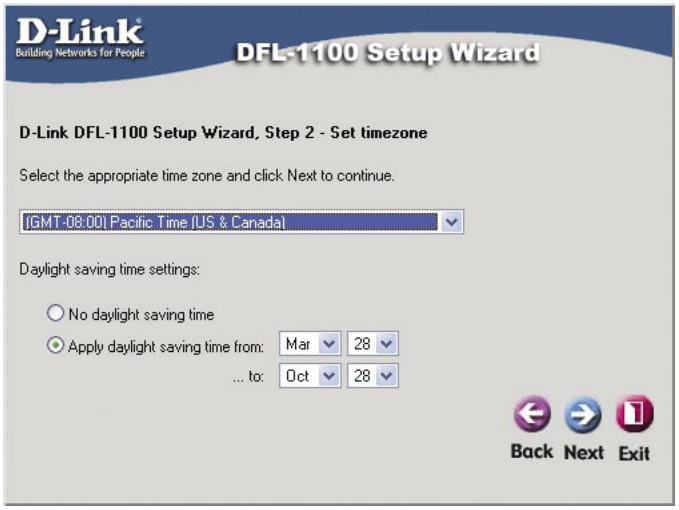
Etape 1 – Création du mot de passe pour admin

Saisissez un mot de passe pour le compte admin puis re-saisissez-le pour confirmer. Cliquez sur **« Next » (Suivant)** pour continuer.



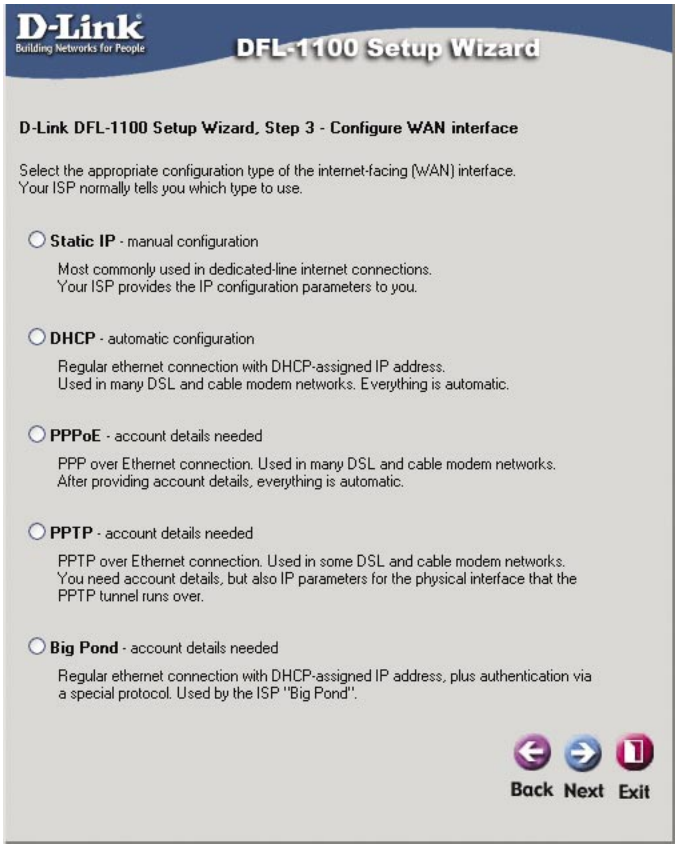
Etape 2 – Définition du fuseau horaire

Choisissez votre fuseau horaire ainsi que les paramètres de passage à l'heure d'été/heure d'hiver. Cliquez sur **« Next » (Suivant)** pour continuer.



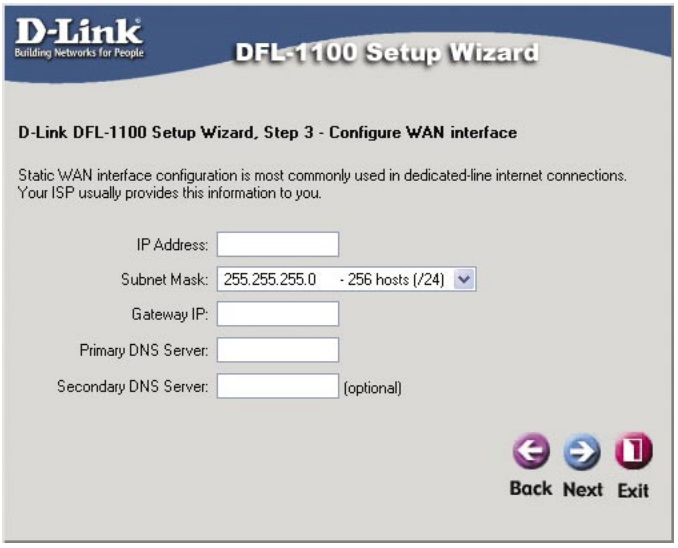
Etape 3 – Configuration de l'interface WAN

Choisissez le the type de connexion à Internet dont vous disposez. En cas de doute, veuillez prendre contact avec votre fournisseur d'accès à Internet. Cliquez sur **« Next » (Suivant)** pour continuer. Si vous avez choisi DHCP, poursuivez à l'étape 4 en page 8.



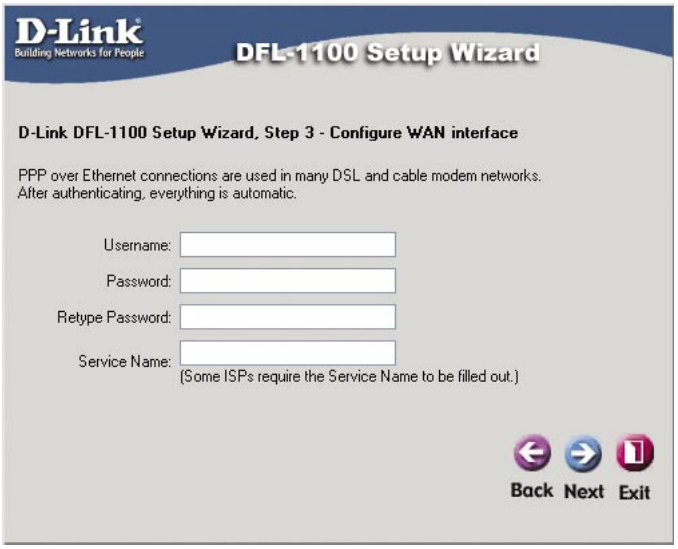
Etape 3 - IP statique

Si vous avez choisi IP statique, saisissez les informations relatives à l'adresse IP qui vous a été communiquée par votre fournisseur d'accès à Internet. Vous devez renseigner tous les champs à l'exception du serveur de DNS secondaire. Cliquez sur **« Next » (Suivant)**. La procédure se poursuit avec l'étape 4 en page 8.



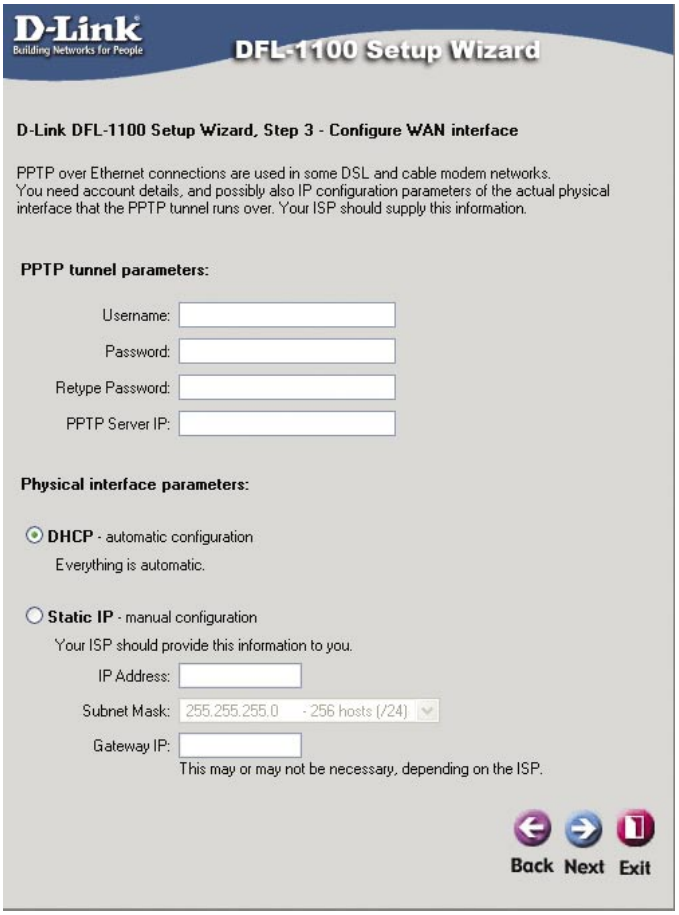
Etape 3 - PPPoE

Si vous avez choisi PPPoE, il vous faut remplir le nom d'utilisateur et le mot de passe qui vous ont été communiqués par votre fournisseur d'accès à Internet. Sauf indication contraire de la part de votre fournisseur d'accès à Internet, veuillez laisser vide le champ Nom de service PPPoE. Cliquez sur **« Next » (Suivant)**. La procédure se poursuit avec l'étape 4 en page 8.



Etape 3 - PPTP

Si vous avez choisi PPTP, il vous faut indiquer les paramètres du tunnel ainsi que ceux de l'interface physique. Cliquez sur **« Next » (Suivant)**. La procédure se poursuit avec l'étape 4 en page 8.



Etape 3 - Big Pond

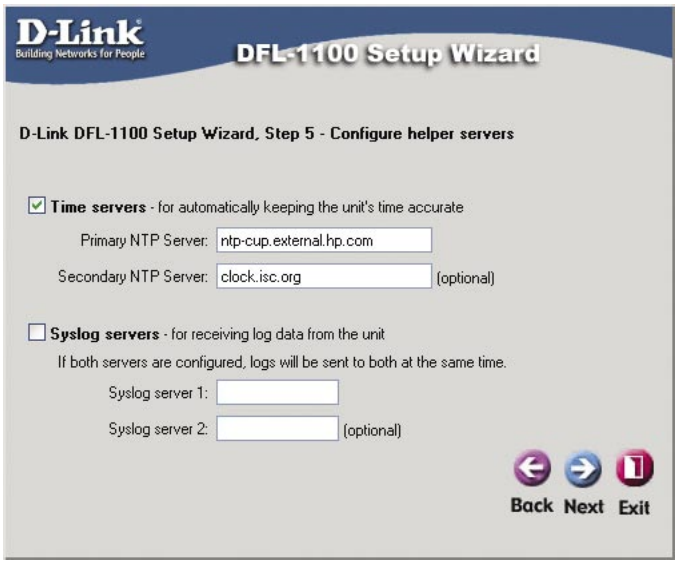
Si vous avez choisi Big Pond, indiquez votre nom d'utilisateur et votre mot de passe, puis re-saisissez votre mot de passe. Il s'agit d'informations que vous a communiquées votre fournisseur d'accès à Internet. Cliquez sur **« Next » (Suivant)** pour continuer.

Etape 4 – Paramétrage du serveur DHCP intégré

- **Disable DHCP Server (Désactiver serveur DHCP) :** Si cette option est désactivée, les clients sur le réseau local doivent être configurés manuellement avec une adresse IP.
- **Enable DHCP Server (Activer serveur DHCP) :** Si cette option est activée, le DFL-1100 attribue automatiquement les informations IP nécessaires à tous les clients sur le réseau local configurés pour DHCP. Le paramètre « IP range » (Intervalle d'adresses IP) définit la première et la dernière adresse de l'intervalle dont sont extraites les adresses attribuées aux clients.

  Assurez-vous que le paramètre « IP range » (Intervalle d'adresses IP) n'entre pas en conflit avec l'adresse IP d'un des éléments du réseau configurés manuellement, y compris celle du DFL-1100.

Etape 5 - Configuration des serveurs auxiliaires

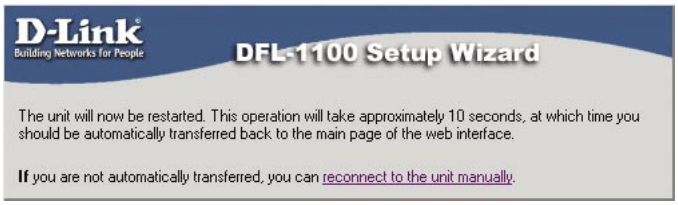


- **Serveurs temporels :** Si cette option est activée, l'heure du pare-feu sera synchronisée par les serveurs NTP dont le nom est saisi.
- **Serveurs Syslog:** Si cette option est activée, le DFL-1100 consignera les données sur les serveurs indiqués.

Assistant d'installation terminé

Cliquez sur **« Restart » (redémarrer)** pour achever la configuration.

Le message qui apparaît indique que l'unité s'apprête à redémarrer.



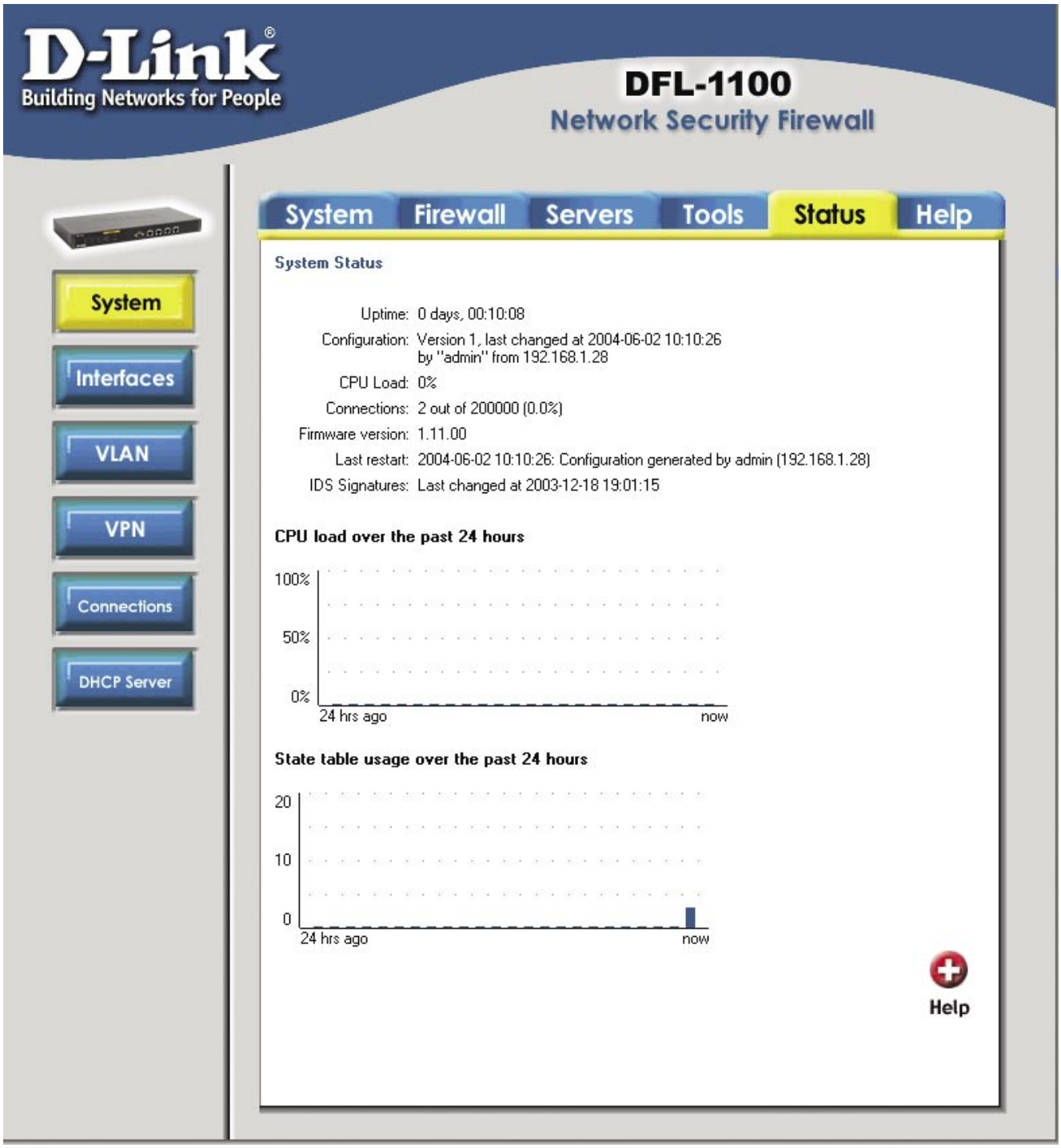
Une fois l'unité configurée, il vous faut vous reconnecter à l'interface de navigation web. Saisissez **https://192.168.1.1**

Veillez à ne pas omettre le « **s** » de « **https** ».

Saisissez admin comme nom d'utilisateur ainsi que le mot de passe que vous avez défini dans l'assistant d'installation.

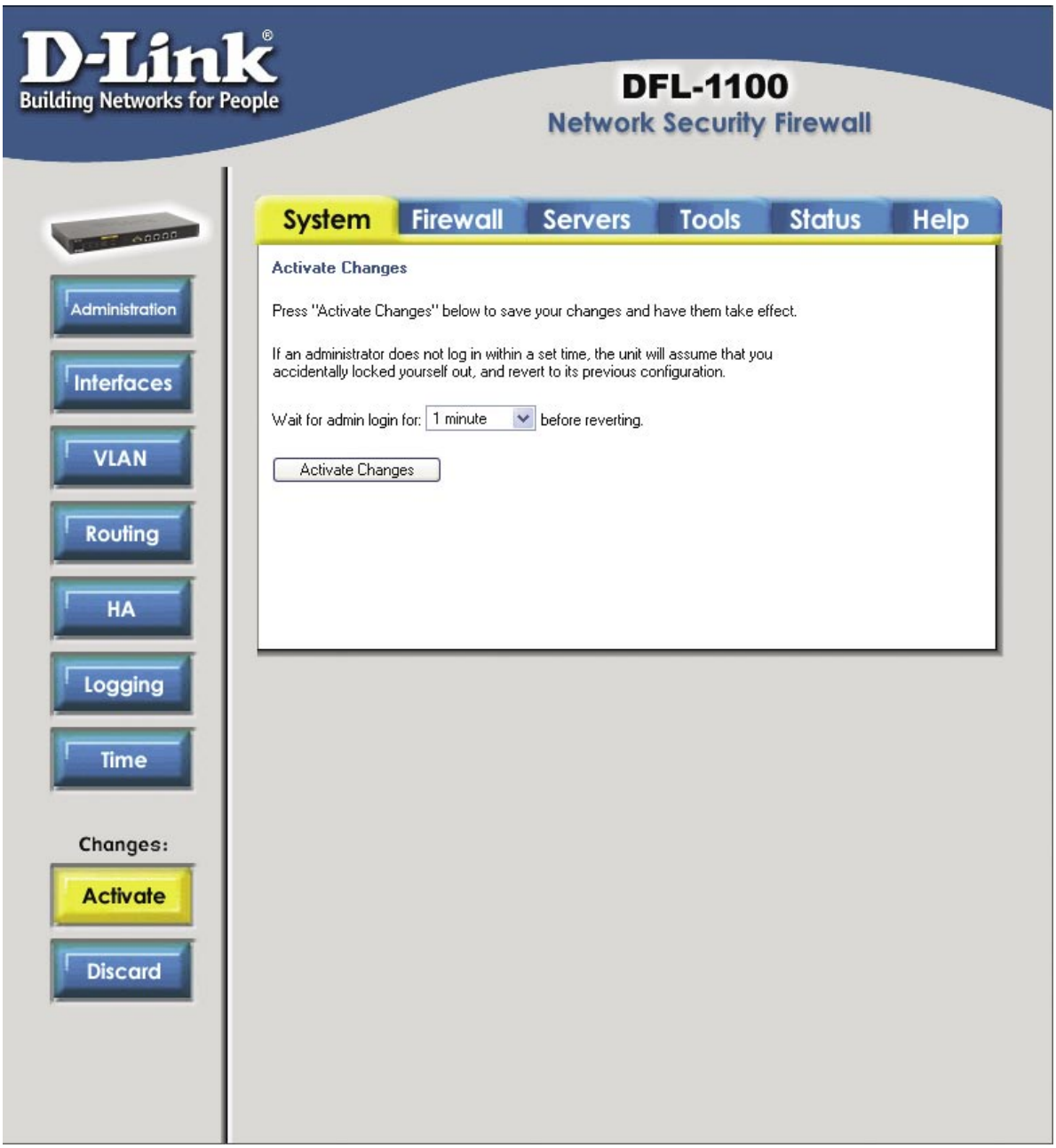
L'installation est achevée!

Une fois reconnecté au DFL-1100, vous devez voir l'écran d'état du système.



Mise en service des modifications sur le D-Link® DFL-1100

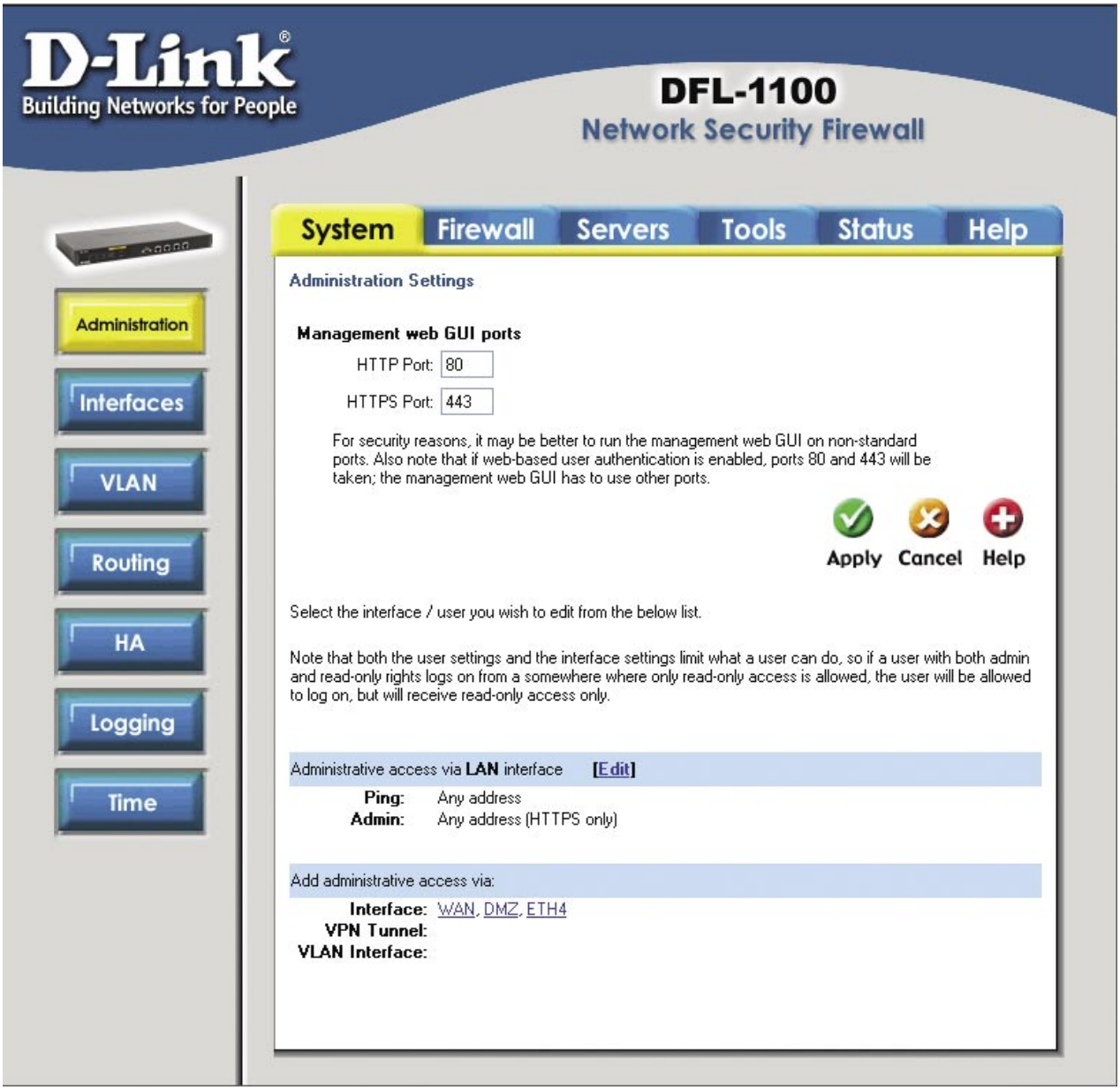
Lorsque des modifications ont été apportées à la configuration du DFL-1100, deux nouveaux boutons apparaissent sous les boutons du menu existants. Une fois tous les changements de paramètres du DFL-1100 effectués, cliquez sur le bouton **« Activate » (Mettre en service)** pour vous rendre à la fenêtre de mise en service des modifications. Une fois les changements validés, l'utilisateur admin doit se reconnecter avant l'expiration de la temporisation dont la durée est définie sur cette page. A défaut, les modifications seront perdues et c'est le paramétrage antérieur qui prévaudra. Une fois que vous avez défini la valeur de la temporisation, cliquez sur le bouton **« Activate Changes » (Mettre en service les modifications)** pour mettre en service les changements de paramétres. Le DFL-1100 enregistre les paramètres, les recharge avant de prendre les modifications en compte. Pour garantir la pérenité des modifications, il faut vous connecter au compte admin avant l'expiration de la temporisation définie plus haut.



Paramétres d'administration

L'écran des paramètres d'administration s'atteint en cliquant sur l'onglet **« System » (Système)** et en choisissant le bouton **« Administration » (Administration)**. Par défaut, l'accès administratif se limite à l'interface **LAN**. C'est le choix que vous avez effectué dans l'assistant d'installation qui détermine si vous pouvez utiliser à la fois **HTTP et HTTPS** pour accéder au DFL-1100 ou si seul **HTTPS** peut être employé. Des interfaces supplémentaires peuvent être configurées pour être accessibles en vue de l'administration en sélectionnant l'interface qui convient (WAN, DMZ ou ETH4).

Ports web de gestion de l'interface utilisateur : il s'agit des ports HTTP et HTTPS qu'utilise le DFL-1100 pour la configuration web. Les paramètres par défaut sont les ports standard : le 80 pour http et le 443 pour HTTPS. Pour des raisons de sécurité, vous pouvez utiliser des numéros de ports non standard.

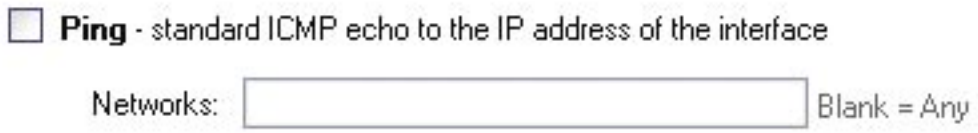


Vous pouvez ajouter, de manière sélective, ajouter des fonctions d'administration à l'une des interfaces. Pour ce faire, cliquez sur l'interface souhaitée (WAN, DMZ ou ETH4) sous l'intitulé : **Add administrative access via: (Ajouter accès administratif via)** ou cliquez sur Edit en regard d'une interface déjà paramétrée.

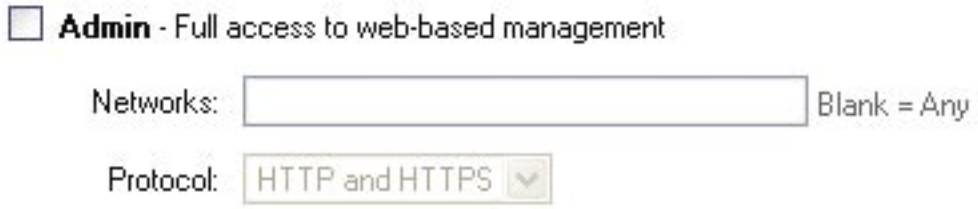
Remarque : les paramètres utilisateur et les paramètres de l'interface limitent la marge de manœuvre de l'utilisateur. Par conséquent, si un véritable administrateur se connecte à travers une interface configurée pour la lecture seule, il sera limité par un accès en lecture seule.

N'importe lequel des paramètres décrits ci-dessous peut être limité à certaines adresses IP particulières (192.168.0.0/24, 10.0.0.5 - 10.0.0.9). Pour cela, il vous suffit de saisir les plages concernées dans le champ **Networks: (Réseaux)**. Si vous laissez ce champ vide, cela signifie qu'il n'y a aucune limitation concernant les adresses IP concernées.

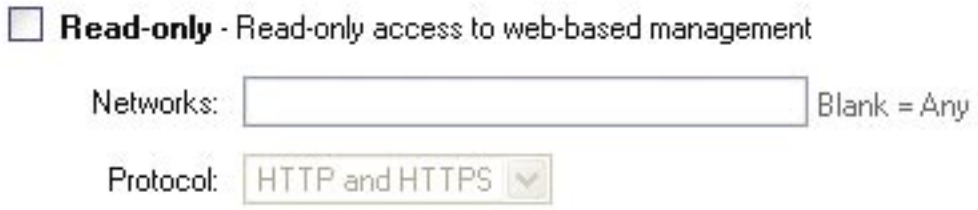
Ping : si ce paramètre est activé, il spécifie les adresses/la plage d'adresses IP qui peuvent faire un « ping » vers l'interface du DFL-1100. Par défaut, tout utilisateur peut effecter un ping vers l'IP de l'interface.



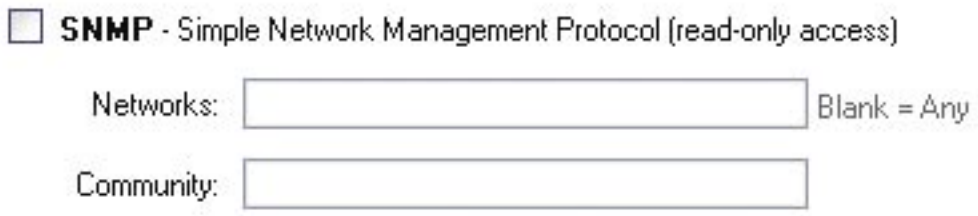
Admin : si ce paramètre est activé, les utilisateurs bénéficiant des droits d'administration peuvent accéder à l'interface spécifiée et disposer d'un accès total à la configuration web. Il est également possible d'autoriser la configuration via **HTTP et HTTPS** ou uniquement via **HTTPS**.



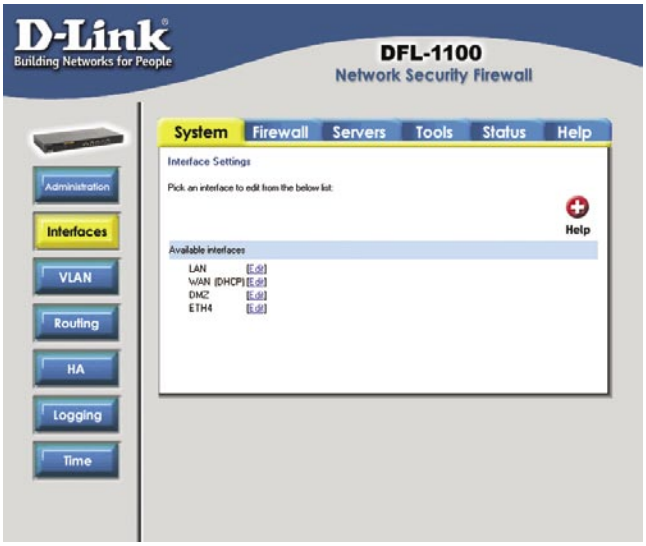
Read-Only (lecture seule) : si ce paramètre est activé, il permet aux utilisateurs de visualiser la configuration du DFL-1100, sans pour autant la modifier, depuis l'interface spécifiée. Il est également possible d'autoriser la visualisation via **HTTP et HTTPS** ou uniquement via **HTTPS**.



SNMP : spécifie si SNMP doit être ou non autorisé pour l'interface spécifiée. Le DFL-1100 permet l'accès en lecture seule.

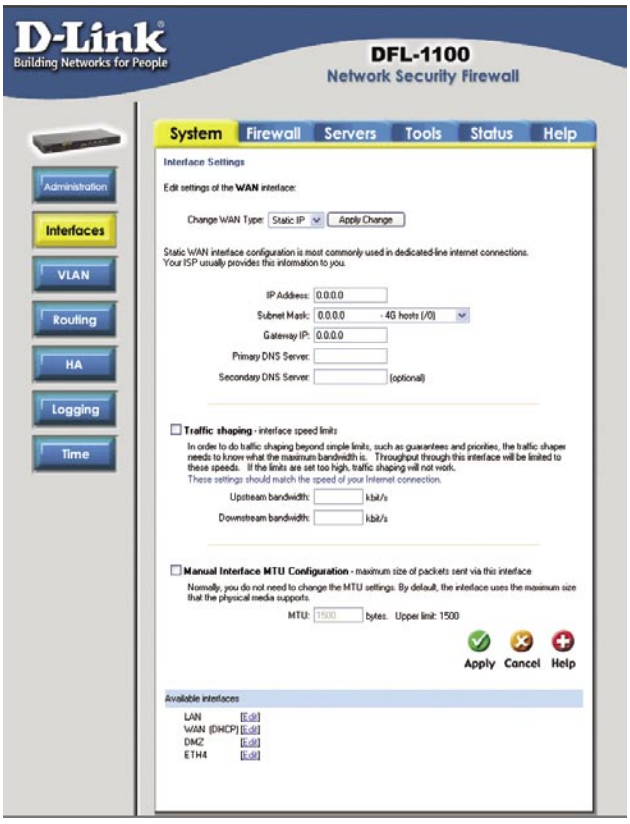


Paramètres de l'interface WAN



Lorsque vous vous connectez au DFL-1100 pour la première fois, l'assistant d'installation vous guide à travers la procédure de configuration des paramètres de base du pare-feu. C'est à ce moment-là que vos paramètres WAN sont configurés. Si vous avez besoin de les modifier, allez à l'onglet **System (Système)** et cliquez sur le bouton **Interfaces (Interfaces)**. Cliquez sur l'option **Edit (Modifier)** située en regard de WAN.

IP statique



IP Address (adresse IP) : l'adresse IP de l'interface WAN. Il s'agit de l'adresse utilisée pour faire un « ping » vers le pare-feu et télécommander ce dernier. Elle sert exactement d'adresse source pour les connexions converties dynamiquement.

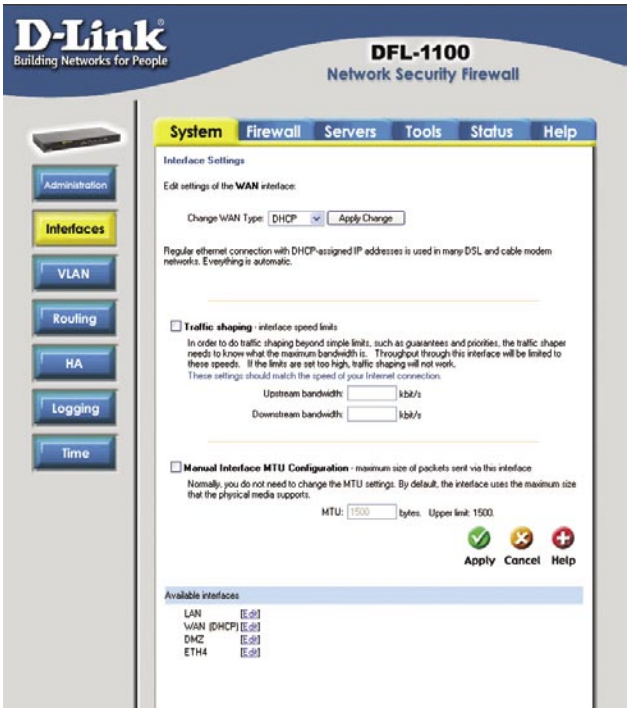
Subnet Mask (masque de sous-réseau) : identifiant du réseau et du sous-réseau.

Gateway IP (IP de la passerelle) : spécifie l'adresse IP de la passerelle par défaut utiliser pour atteindre Internet.

Primary and Secondary DNS Server (serveur de DNS primaire et secondaire) : la ou les adresses IP de votre ou vos serveur(s) de DNS. Seul le serveur de DNS primaire est obligatoire.

DHCP

Si vous utilisez le protocole DHCP, vous n'avez aucun paramètre à saisir.



PPPoE

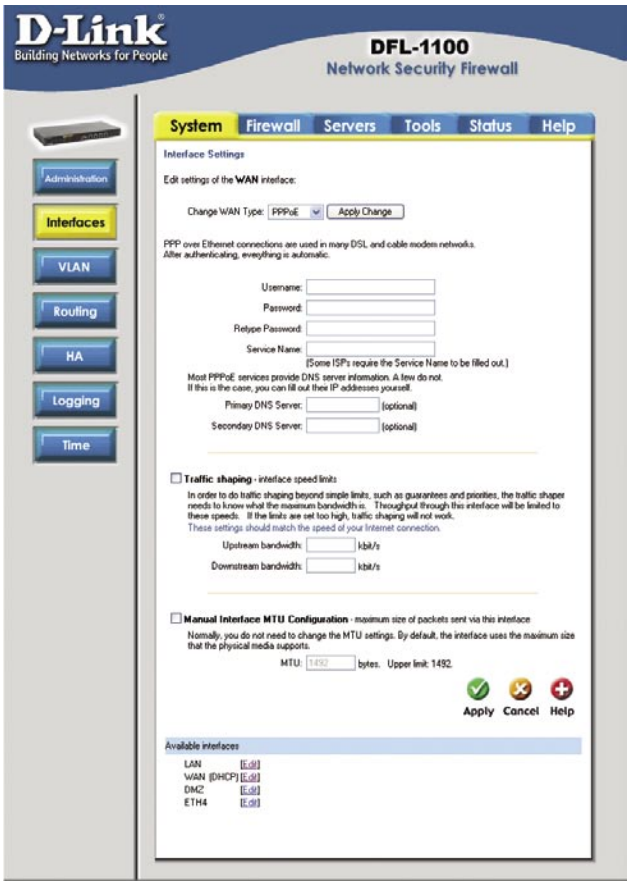
Si vous utilisez une connexion PPPoE, vous devez saisir le nom d'utilisateur et le mot de passe, re-saisir le mot de passe, puis saisir les autres informations exigées par votre fournisseur d'accès à Internet (FAI), le cas échéant.

Username (nom d'utilisateur) : le nom d'utilisateur que vous a indiqué votre FAI pour vous connecter.

Password (mot de passe) : le mot de passe associé à votre nom d'utilisateur.

Service Name (nom de service) : cette option ne doit être utilisée que si votre FAI l'exige. Dans ce cas, il vous aura indiqué le nom de service à saisir ici.

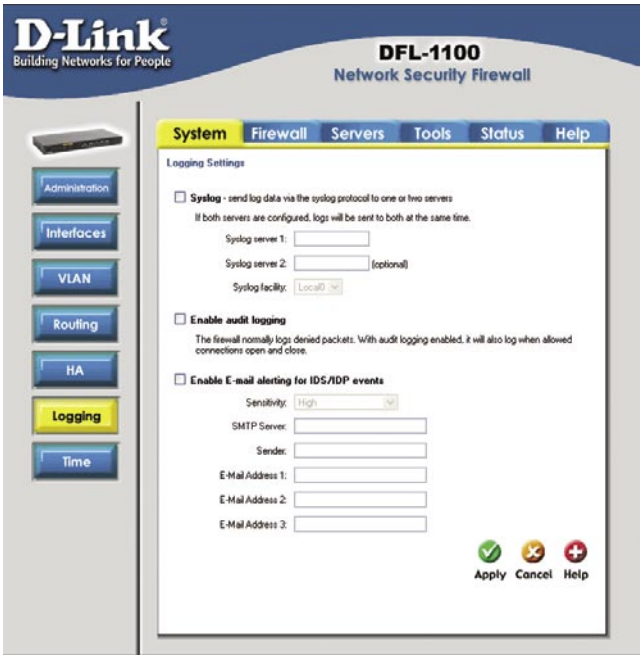
Primary and Secondary DNS Server (serveur de DNS primaire et secondaire) : les adresse IP de vos serveurs de DNS. Celles-ci sont facultatives et généralement communiquées par le service PPPoE.



Consignation

Pour vous rendre à l'écran de configuration de la consignation, sélectionnez l'onglet **System (système)** et cliquez sur le bouton **Logging (consignation)**.

La consignation vous permet de garder trace d'événements tels que le démarrage, l'arrêt, l'ouverture et la clôture des connexions. Les événements de démarrage et d'arrêt sont systématiquement consignés. La consignation d'événements tels que l'ouverture ou la clôture de connexions autorisées est configurable par l'utilisateur. Le DFL-1100 envoie les données du journal vers un ou deux serveurs Syslog. Une alerte par e-mail concernant les événements IDS/IDP peut être générée pour un maximum de trois adresses e-mail.



Activation de la consignation

1. Cochez la case Syslog.
2. Saisissez le nom de votre premier serveur Syslog dans la zone de texte **Syslog server 1 (serveur Syslog 1)**. Si vous avez un second serveur Syslog, saisissez son nom dans la zone de texte Syslog server 2 (serveur Syslog 2). Pour que la consignation puisse fonctionner, vous devez avoir saisi au moins un serveur Syslog.
3. Indiquez quelle installation doit être utilisée en sélectionnant l'installation Syslog correspondante. L'installation Syslog permet d'identifier d'où provient un message. La valeur de l'installation est utilisée par le PC sur lequel s'exécute le Démon Syslog pour trier les messages. **Local0** est la valeur par défaut, dans la mesure où il s'agit de la valeur généralement attribuée aux pare-feu.
4. Cliquez sur **Apply (Appliquer)** pour appliquer les paramètres, ou cliquez sur **Cancel (Annuler)** pour ne pas tenir compte des modifications.

Activation de la consignation d'audit

Pour commencer à auditer l'ensemble du trafic sur votre pare-feu, il vous suffit de sélectionner la case à cocher **Enable audit logging (Activer la consignation d'audit)**. N'oubliez pas de cliquer sur **Apply (Appliquer)** pour appliquer le paramètre. Sinon, vous pouvez cliquer sur **Cancel (Annuler)** pour ne pas tenir compte de cette modification.

Activation des alertes par e-mail pour les événements IDS/IDP

1. Sélectionnez l'option **Enable E-mail alerting for IDS/IDP events (Activer les alertes par e-mail pour les événements IDS/IDP).**
2. Sélectionnez un degré de Sensitivity (sensibilité). Cinq niveaux de sensibilité vous sont proposés pour le reporting IDS/IDP par e-mail : le niveau supérieur (Very High) vous enverra une alerte par e-mail à la moindre attaque dans le fichier de signature IDS. Les niveaux de sensibilité inférieurs permettent de réduire le nombre d'alertes par e-mail sans pour autant amoindrir la protection IDS.
3. Dans le champ SMTP Server (serveur SMTP), tapez l'adresse du serveur SMTP que doit utiliser le DFL-1100 pour envoyer des e-mails.
4. Le DFL-1100 peut envoyer les alertes par e-mail à un maximum de 3 adresses en cours de validité. Saisissez ces adresses dans la zone de texte correspondante.
5. Cliquez sur **Apply (Appliquer)** pour appliquer les paramètres, ou cliquez sur **Cancel (Annuler)** pour ne pas tenir compte des modifications.

Heure

L'écran de configuration de l'heure s'affiche si vous sélectionnez l'onglet **System (Système)** puis cliquez sur le bouton **Time (Heure)**. L'heure peut être réglée manuellement ou synchronisée par rapport à un serveur d'heure réseau sur Internet.

Modification du fuseau horaire

1. Sélectionnez le fuseau horaire qui vous correspond dans le menu déroulant.
2. Spécifiez vos paramètres de passage à l'heure d'été ou indiquez que vous n'avez pas de passage à l'heure d'été en sélectionnant le bouton correspondant.
3. Cliquez sur **Apply (Appliquer)** pour appliquer les paramètres, ou cliquez sur **Cancel (Annuler)** pour ne pas tenir compte des modifications.

Utilisation de NTP pour synchroniser l'heure

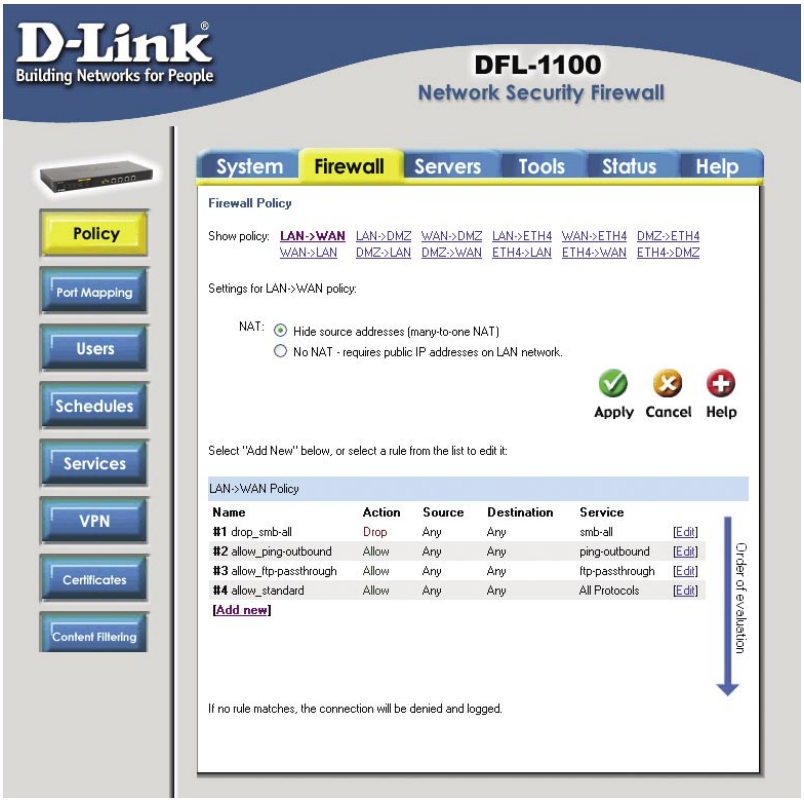
1. Activez la synchronisation en sélectionnant la case à cocher Enable NTP (Activer NTP).
2. Saisissez l'adresse IP ou le nom du serveur avec lequel vous souhaitez vous synchroniser.
3. Cliquez sur **Apply (Appliquer)** pour appliquer les paramètres, ou cliquez sur **Cancel (Annuler)** pour ne pas tenir compte des modifications.

Réglage manuel de l'heure et de la date

1. Sélectionnez la case à cocher **Set the system time (Régler l'heure système).**
2. Sélectionnez la date qui convient dans les listes déroulantes.
3. Saisissez l'heure qui convient au format 24 heures.
4. Cliquez sur **Apply (Appliquer)** pour appliquer les paramètres, ou cliquez sur **Cancel (Annuler)** pour ne pas tenir compte des modifications.

Politique de pare-feu

Le DFL-1100 vous permet de configurer des politiques pour gérer les données émises et reçues à travers les différentes interfaces. La fenêtre de configuration de politique apparaît si vous allez dans l'onglet **Firewall (Pare-feu)** et que le bouton **Policy (Politique)** est la sélection par défaut.



Ajout d'une nouvelle politique

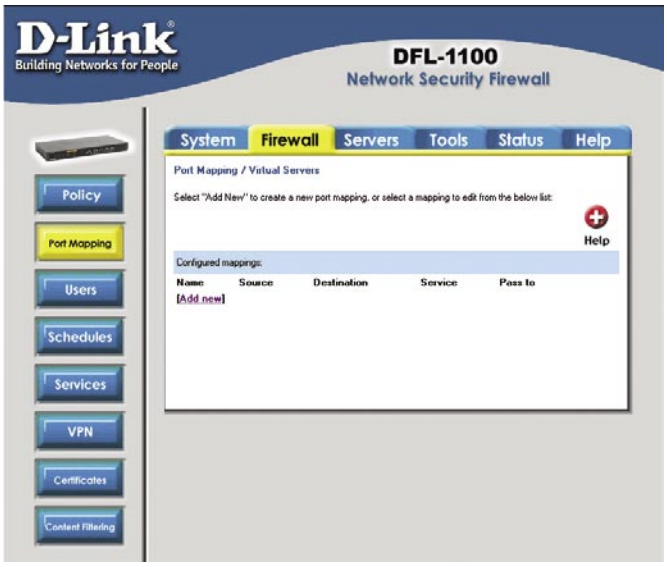
1. Sélectionnez les interfaces désirées pour créer une politique. Par exemple, **LAN > WAN** crée une politique pour les données provenant du réseau local interne qui sont transmises vers Internet.
2. Cliquez sur le lien **Add new (Ajouter nouvelle)**.
3. Saisissez les valeurs correspondant aux options décrites ci-dessous :

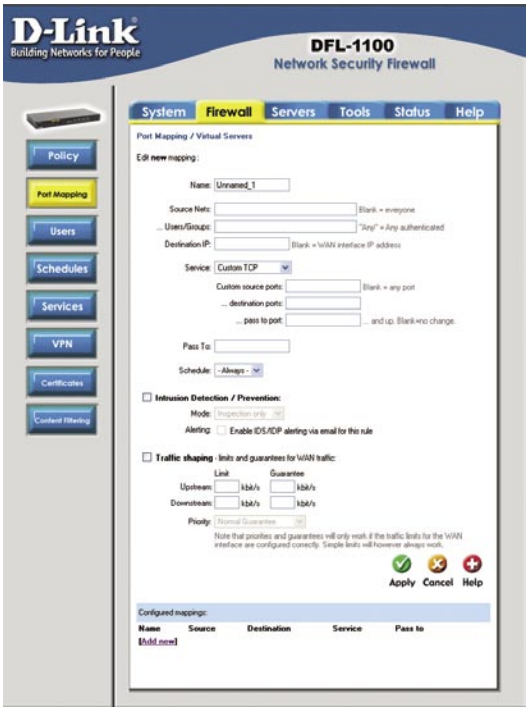
Name (Nom)	Créez le nom de la politique. Ce nom sert essentiellement de référence de règle dans les données de journal. Il permet également de se repérer facilement dans la liste des politiques.
Action (Action)	Sélectionnez l'action à exécuter avec les données spécifiées.
Source Nets (Réseaux sources)	Spécifie la plage d'adresses IP de l'émetteur, à comparer avec le paquet reçu. Pour que tout corresponde, laissez ce champ vide.
Source Users/Groups (Utilisateurs/Groupes sources)	Ici vous pouvez spécifiquer qu'un nom d'utilisateur, un groupe ou tout autre utilisateur authentifié doit être la source pour que l'action puisse se produire. Vous pouvez saisir une liste de noms d'utilisateurs, séparés par une virgule, ou indiquer « Any » (quelconque) pour représenter n'importe quel utilisateur authentifié. Si ce champ est laissé vide, la politique considérée n'exige pas d'authentification.
Destination Nets (Réseaux destinataires)	Spécifie la plage d'adresses IP à comparer avec l'IP de destination du paquet reçu. Pour que tout corresponde, laissez ce champ vide.
Destination Users/Groups (Utilisateurs/Groupes destinataires)	Vous pouvez utiliser un nom d'utilisateur spécifique auquel doit correspondre cette politique. Vous pouvez saisir une liste de noms d'utilisateurs, séparés par une virgule, ou indiquer « Any » (quelconque) pour représenter n'importe quel utilisateur authentifié. Si ce champ est laissé vide, la politique considérée n'exige pas d'authentification.
Service (Service)	Vous pouvez sélectionner un service prédéfini dans le menu déroulant. Sinon, vous pouvez créer un service personnalisé.
Schedule (Calendrier)	Sélectionnez le calendrier selon lequel cette politique doit correspondre. Choisissez Always (Toujours) pour qu'il n'y ait aucune planification.

4. Cliquez sur **Apply (Appliquer)** pour appliquer les paramètres, ou cliquez sur **Cancel (Annuler)** pour ne pas tenir compte des modifications.

Mappage de ports / Serveurs virtuels

La section de configuration Port Mapping / Virtual Servers (Mappage de ports / Serveurs virtuels) vous permet de configurer des serveurs virtuels tels que des serveurs web. Les mappages sont lus de haut en bas. Le premier mappage qui correspond est effectué. L'écran de configuration Port Mapping / Virtual Servers (Mappage de ports / Serveurs virtuels) apparaît si vous allez à l'onglet **Firewall (Pare-feu)** et que vous cliquez sur le bouton **Port Mapping (Mappage de ports).**





Ajout d'un nouveau mappage

1. Cliquez sur le lien **Add new** **(Ajouter nouveau)**.
2. Renseignez les paramètres suivants :

Name (Nom)	Créez le nom de la politique. Ce nom sert essentiellement de référence de règle dans les données de journal. Il permet également de se repérer facilement dans la liste des politiques.
Action (Action)	Sélectionnez l'action à exécuter avec les données spécifiées.
Source Nets (Réseaux sources)	Spécifie la plage d'adresses IP de l'émetteur, à comparer avec le paquet reçu. Pour que tout corresponde, laissez ce champ vide.
Source Users/Groups (Utilisateurs/Groupes sources)	Ici vous pouvez spécifiquer qu'un nom d'utilisateur, un groupe ou tout autre utilisateur authentifié doit être la source pour que l'action puisse se produire. Vous pouvez saisir une liste de noms d'utilisateurs, séparés par une virgule, ou indiquer « Any » (quelconque) pour représenter n'importe quel utilisateur authentifié. Si ce champ est laissé vide, la politique considérée n'exige pas d'authentification.
Destination Nets (Réseaux destinataires)	Spécifie la plage d'adresses IP à comparer avec l'IP de destination du paquet reçu. Pour que tout corresponde, laissez ce champ vide.
Destination Users/Groups (Utilisateurs/Groupes destinataires)	Vous pouvez utiliser un nom d'utilisateur spécifique auquel doit correspondre cette politique. Vous pouvez saisir une liste de noms d'utilisateurs, séparés par une virgule, ou indiquer « Any » (quelconque) pour représenter n'importe quel utilisateur authentifié. Si ce champ est laissé vide, la politique considérée n'exige pas d'authentification.
Service (Service)	Vous pouvez sélectionner un service prédéfini dans le menu déroulant. Sinon, vous pouvez créer un service personnalisé.
Schedule (Calendrier)	Sélectionnez le calendrier selon lequel cette politique doit correspondre. Choisissez Always (Toujours) pour qu'il n'y ait aucune planification.

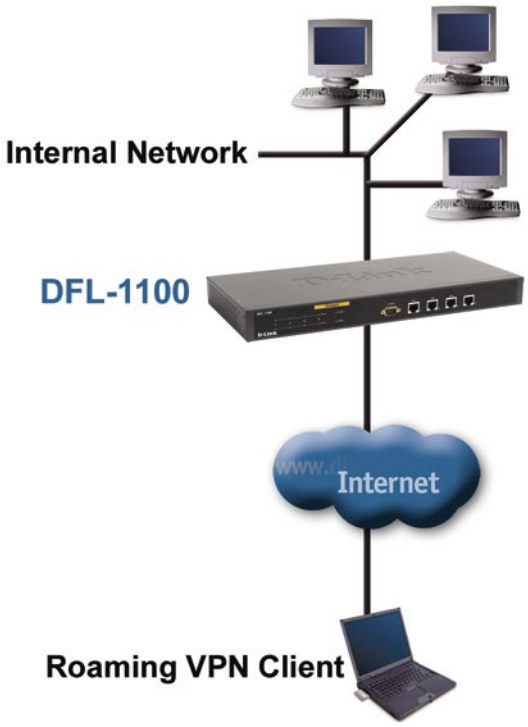
4. Si vous utilisez le Traffic Shaping (Définition de forme du trafic), saisissez les informations correspondantes. Sinon, vous pouvez sauter cette étape.
5. Cliquez sur **Apply (Appliquer)** pour appliquer les paramètres, ou cliquez sur **Cancel (Annuler)** pour ne pas tenir compte des modifications.

Configuration du VPN IPSec

L'écran de configuration du VPN apparaît si vous allez à l'onglet **Firewall (Pare-feu)** et sélectionnez le bouton **VPN**.

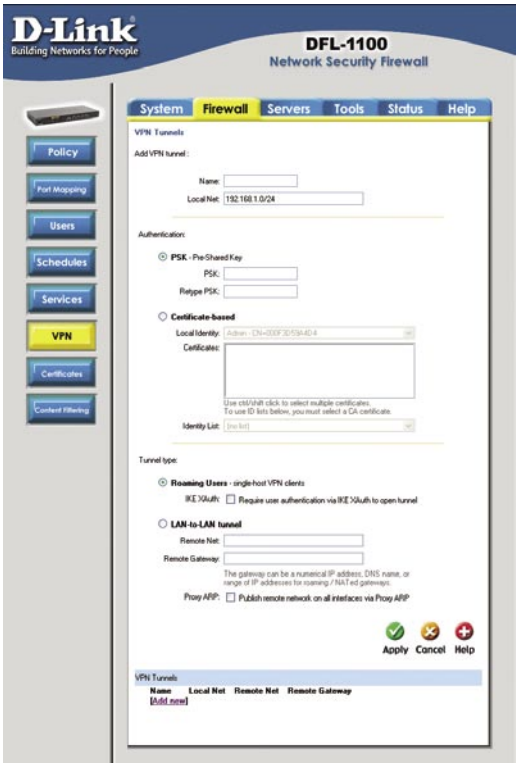
VPN IPSec entre un client et un réseau interne

Les utilisateurs peuvent se connecter au réseau interne du siège à partir de n'importe quelle connexion à Internet. La communication entre le client et le réseau interne se fait à travers un tunnel VPN crypté qui relie le DFL-1100 aux utilisateurs nomades répartis sur Internet. Le client peut se connecter à un réseau interne ou au réseau DMZ.



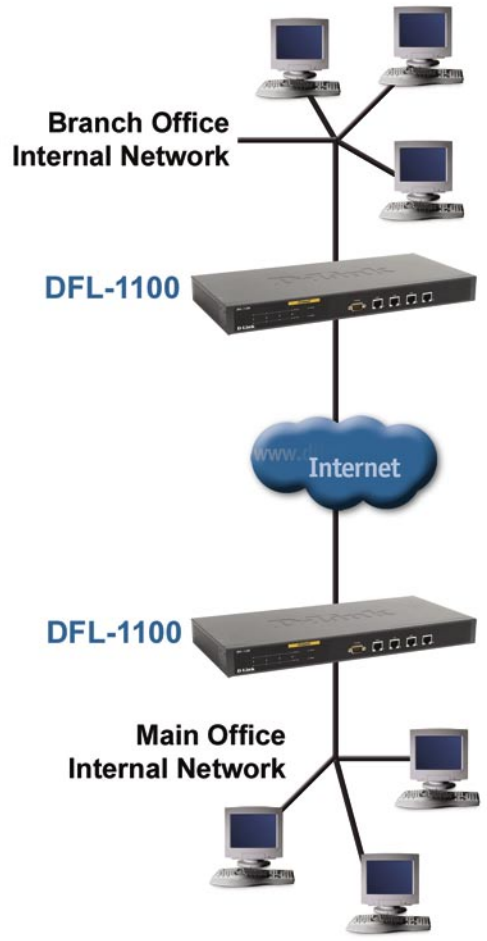
Création d'un tunnel VPN pour les utilisateurs nomades

1. Cliquez sur le lien **Add new** **(Ajouter nouveau)**.
2. Saisissez le nom du nouveau tunnel dans le champ de nom. Ce nom peut comporter des chiffres (**0-9**), des lettres majuscules ou minuscules (**A-Z, a-z**), des barres obliques (**-**) et des traits soulignés (**_**).
3. Dans le champ Local Net (réseau local), saisissez le réseau local auquel doivent se connecter vos clients nomades.
4. Choisissez le type d'authentification : PSK (Pre-shared Key, soit clé pré-partagée) ou Certificate-based (à base de certificat). Si vous sélectionnez PSK, assurez-vous que les clients utilisent la même PSK que vous.
5. Sélectionnez **Roaming Users (Utilisateurs nomades)** en tant que Tunnel Type (type de tunnel).
6. Cliquez sur **Apply (Appliquer)** pour appliquer les paramètres, ou cliquez sur **Cancel (Annuler)** pour ne pas tenir compte des modifications.



VPN IPSec entre deux réseaux

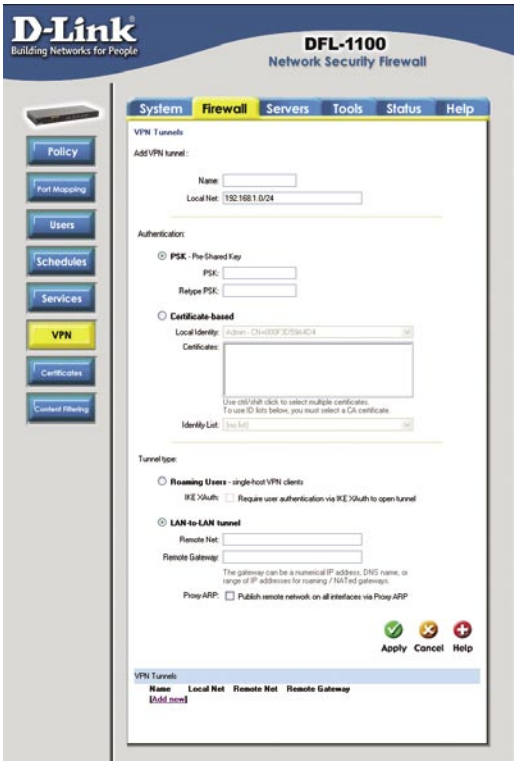
Les utilisateurs peuvent se connecter depuis un réseau interne situé sur un site, vers un autre réseau interne situé sur un autre site, le tout en passant par Internet. La communication entre les deux réseaux se fait dans un tunnel VPN crypté qui relie deux DFL-1100 à travers Internet. Les utilisateurs des réseaux internes ne savent pas qu'ils se connectent à un ordinateur situé sur l'autre réseau : à leurs yeux, la connexion se fait via Internet. Il est possible de se connecter aux connexions LAN internes ou aux connexions DMZ.



Création d'un tunnel VPN « LAN-to-LAN »

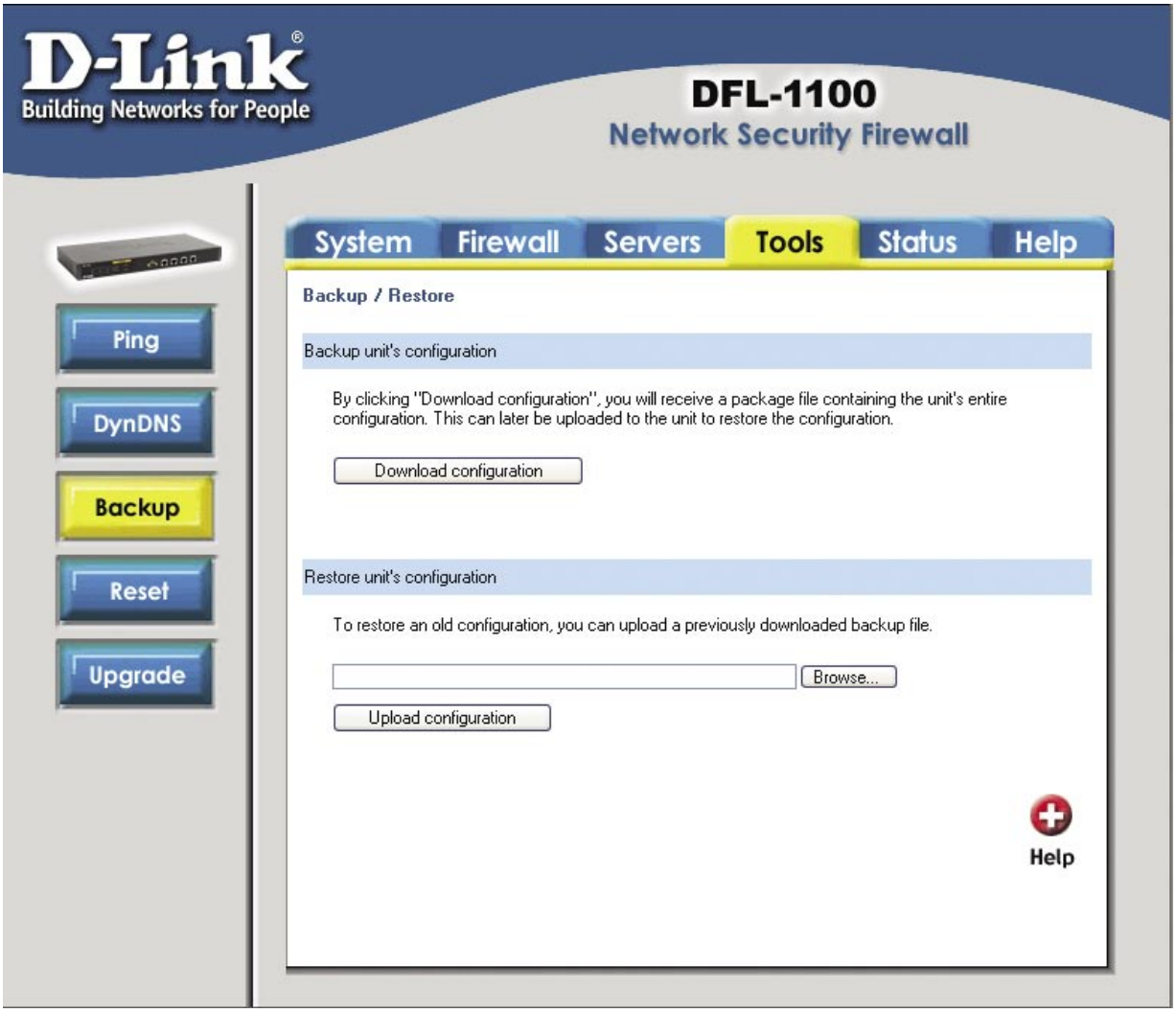
Remarques : cette procédure doit être suivie sur les deux DFL-1100.

1. Cliquez sur le lien **Add new** **(Ajouter nouveau)**.
2. Saisissez le nom du nouveau tunnel dans le champ de nom. Ce nom peut comporter des chiffres (**0-9**), des lettres majuscules ou minuscules (**A-Z, a-z**), des barres obliques (**-**) et des traits soulignés (**_**).
3. Dans le champ Local Net (réseau local), saisissez le réseau local que devra utiliser le tunnel « LAN-to-LAN ».
4. Choisissez le type d'authentification : PSK (Pre-shared Key, soit clé pré-partagée) ou Certificate-based (à base de certificat). Si vous choisissez PSK, assurez-vous que les deux DFL-1100 sont configurés de manière à utiliser la même PSK.
5. Sélectionnez le type de tunnel LAN-to-LAN et spécifiez le réseau situé derrière l'autre DFL-1100 en tant que Remote Net (Réseau distant). Spécifiez l'IP externe de l'autre DFL-1100 par une adresse IP ou un nom de DNS.
6. Cliquez sur **Apply (Appliquer)** pour appliquer les paramètres, ou cliquez sur **Cancel (Annuler)** pour ne pas tenir compte des modifications.



Sauvegarde

Pour atteindre l'écran Backup (Sauvegarde), allez à l'onglet **Tools (Outils)** et sélectionnez le bouton Backup (Sauvegarde). L'option **Backup (Sauvegarde)** permet à l'administrateur de sauvegarder et de rétablir la configuration du DFL-1100. Le fichier de configuration contient les paramètres système, les adresses IP, les tables d'adresses, les tables de service, les paramètres IPSec, les mappages de ports et les politiques. Lorsque votre DFL-1100 est totalement configuré, vous pouvez enregistrer le fichier de configuration sur un disque local. Vous pouvez ensuite à tout moment rétablir la configuration à partir du fichier de configuration situé sur le disque local en question.



Exportation du fichier de configuration

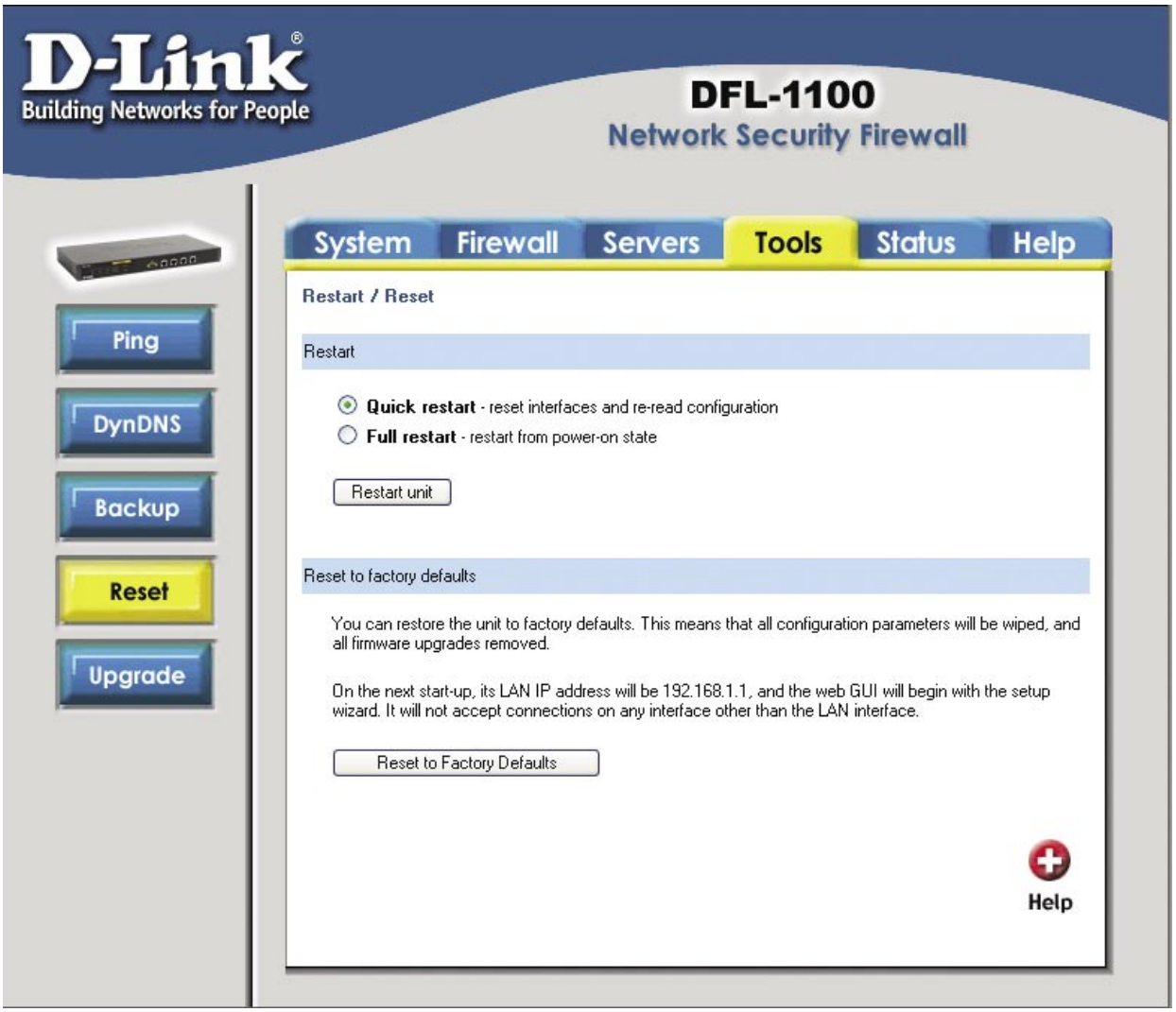
1. Cliquez sur le bouton **Download Configuration (Télécharger la configuration)**.
2. Choisissez un emplacement de destination où enregistrer le fichier de configuration. L'administrateur peut renommer ce fichier s'il le souhaite.

Chargement d'un fichier de configuration préalablement sauvegardé

1. Cliquez sur le bouton Browse (Parcourir), puis repérez et sélectionnez un fichier de configuration préalablement sauvegardé.
2. Cliquez sur le bouton Upload Configuration (Télédécharger la configuration) pour importer le fichier dans le pare-feu.

Redémarrage / Réinitialisation

La fenêtre Restart / Reset (Redémarrage/Réinitialisation) s'affiche si vous allez à l'onglet **Tools (Outils)** et cliquez sur le bouton **Reset (Réinitialisation)**.



Redémarrage du DFL-1100

1. Sélectionnez le redémarrage rapide ou complet. Le redémarrage rapide réinitialise les interfaces et re-lit la configuration. Le redémarrage complet correspond au démarrage de l'appareil après sa mise hors tension.
2. Cliquez sur le bouton **Restart Unit (Redémarrer l'appareil)** pour redémarrer votre DFL-1100.

Rétablissement des paramètres par défaut d'usine

Si vous rétablissez les paramètres système par défaut d'usine, **vous perdez toutes les modifications que vous aviez apportées à la configuration du DFL-1100**. La réinitialisation du système revient également à la version originale du firmware si ce dernier a été modifié. Pour rétablir les paramètres par défaut d'usine, cliquez sur le bouton **Reset to Factory Defaults (Rétablir les paramètres par défaut d'usine).**

Assistance technique

Vous trouverez la documentation et les logiciels les plus récents sur le site web **D-Link**.

Le service technique de **D-Link** est gratuit pour les clients aux Etats-Unis durant la période de garantie.

Ceux-ci peuvent contacter le service technique de
D-Link par notre site internet ou par téléphone.

Assistance technique D-Link par téléphone :
0 820 0803 03

Assistance technique D-Link sur internet :
Web :http://www.dlink.fr
E-mail :support@dlink.fr