et cifom

CPLN Ecole technique

# 03 Le pare-feu

Module 146

ICT Berufsbildung
Formation professionnelle
Formazione professionale

# 1. Introduction

**Terminologie :**

Un pare-feu est parfois appelé coupe-feu, garde-barrière, barrière de sécurité ou encore firewall.

**Origine du terme :**

En informatique l'usage du terme « pare-feu » est donc métaphorique, il évoque une porte empêchant les flammes d'Internet d'entrer chez soi et/ou de « contaminer » un réseau informatique.

Le pare-feu peut être ,

- un programme installé sur un ordinateur.
- un appareil à part entière (e.g. : Cisco ASA 5585-X).
- une service installé sur un routeur «multi-tâches» (e.g. : Zyxel 460N, …)

## 2. Les règles

Un système pare-feu contient un ensemble de règles prédéfinies.

Il permet d'autoriser la connexion, de bloquer la connexion, de rejeter la demande de connexion sans avertir l'émetteur.

- **Allow** : autoriser la connexion
- **Deny :** bloquer la connexion
- **Drop :** rejeter la demande de connexion

On distingue deux types de politiques de sécurité :

- autoriser uniquement les communications ayant été explicitement autorisées ;
- empêcher les échanges qui ont été explicitement interdits.

# 3. Le filtrage

Un système pare-feu fonctionne sur le principe du filtrage simple de paquets.

Les paquets de données, analysés par le pare-feu, possèdent les en-têtes suivantes :

- adresse IP de la machine émettrice;
- adresse IP de la machine réceptrice;
- type de paquet (TCP, UDP, etc.);
- numéro de port.

| Règle | Action | IP source | IP dest | Prot. | Port source | Port dest |
|---|---|---|---|---|---|---|
| 1 | Accept | 192.168.10.20 | 194.154.192.3 | tcp | any | 25 |
| 2 | Accept | any | 192.168.10.3 | tcp | any | 80 |
| 3 | Accept | 192.168.10.0/24 | any | tcp | any | 80 |
| 4 | Deny | any | any | any | any | any |

# 4. Le filtrage dynamique

Le filtrage dynamique de paquets permet d'effectuer un suivi des transactions entre le client et le serveur.

De nombreux services, comme FTP, initient une connexion sur un port statique, mais ouvrent dynamiquement un port afin d'établir une session entre la machine serveur et la machine cliente.

Le filtrage dynamique permet de tenir compte de l'état des anciens paquets pour appliquer les règles de filtrage (OSI 3 et 4).

De cette manière, l'ensemble des paquets transitant dans le cadre de cette connexion seront implicitement acceptés par le pare-feu.

# 5. Le filtrage applicatif

Le filtrage applicatif permet de filtrer les communications application par application (OSI 7).

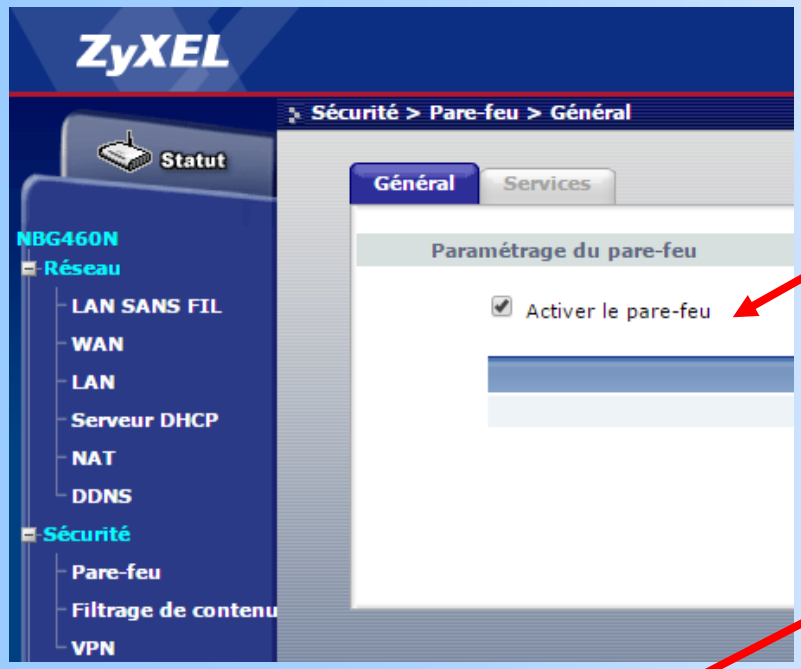
Un firewall effectuant un filtrage applicatif est appelé généralement **passerelle applicative** ou **proxy**.

Il est recommandé de dissocier le pare-feu du proxy, afin de limiter les risques de compromission.

Il faut surveiller le journal d'activité du pare-feu et se tenir au courant des alertes de sécurité.

# 6. Utilisation du routeur Zyxel 460N

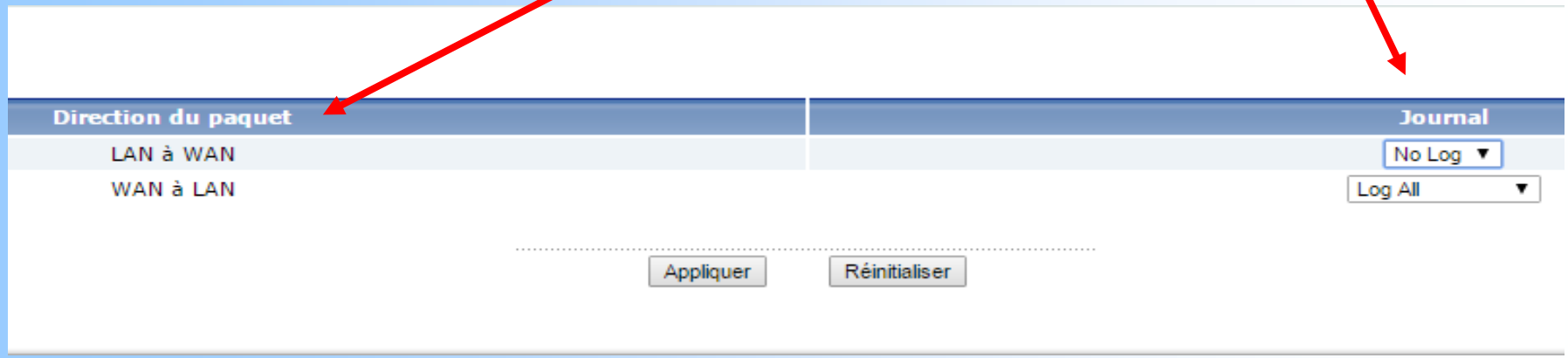
Voyons comment paramétrer le routeur Zyxel :




Le pare-feu est activé par défaut.

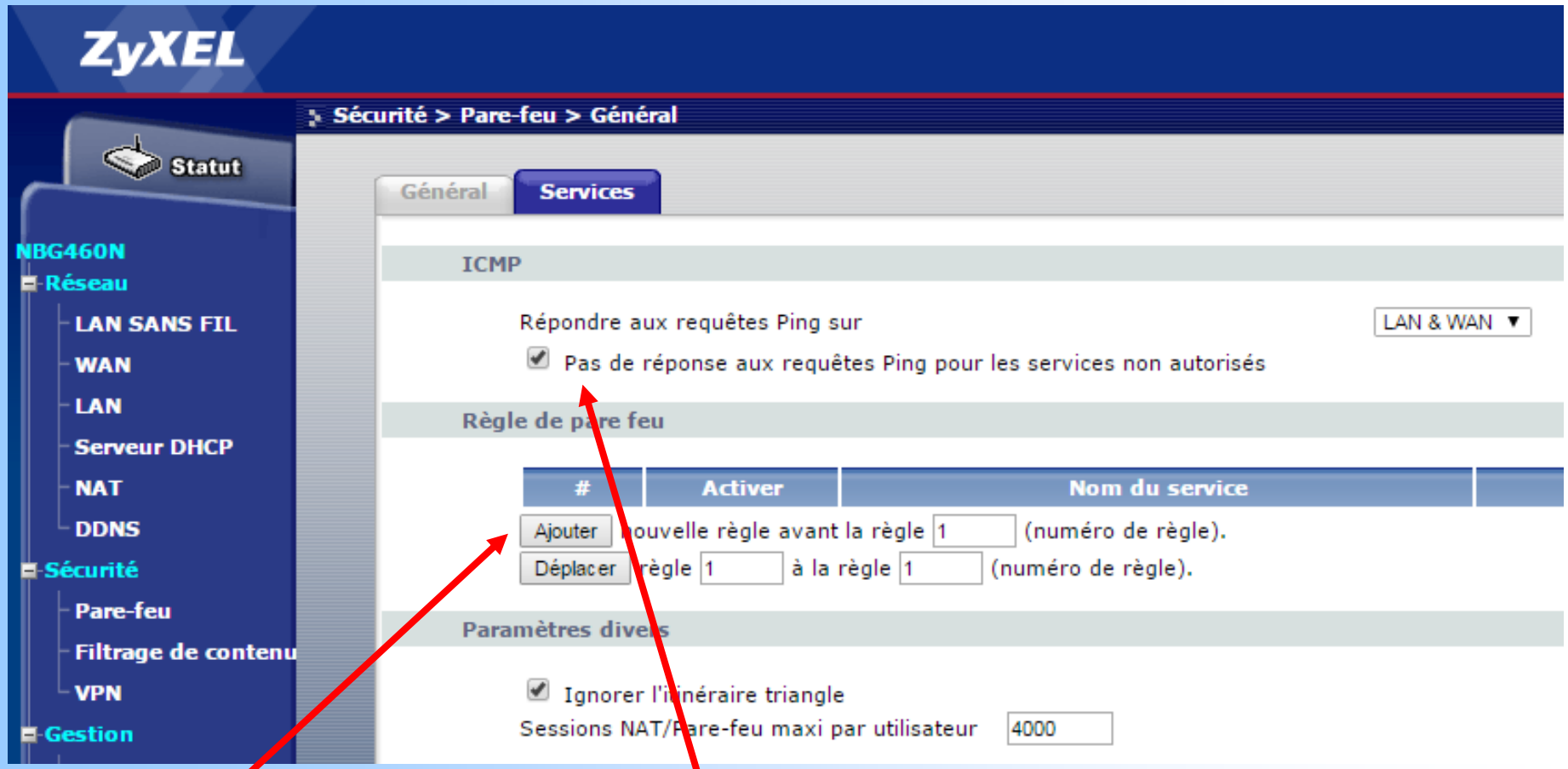
choix de l'activation du journal au log ou non…

… et selon le sens : LAN à WAN ou WAN à LAN.



# 6. Utilisation du routeur Zyxel 460N

Le menu Services :

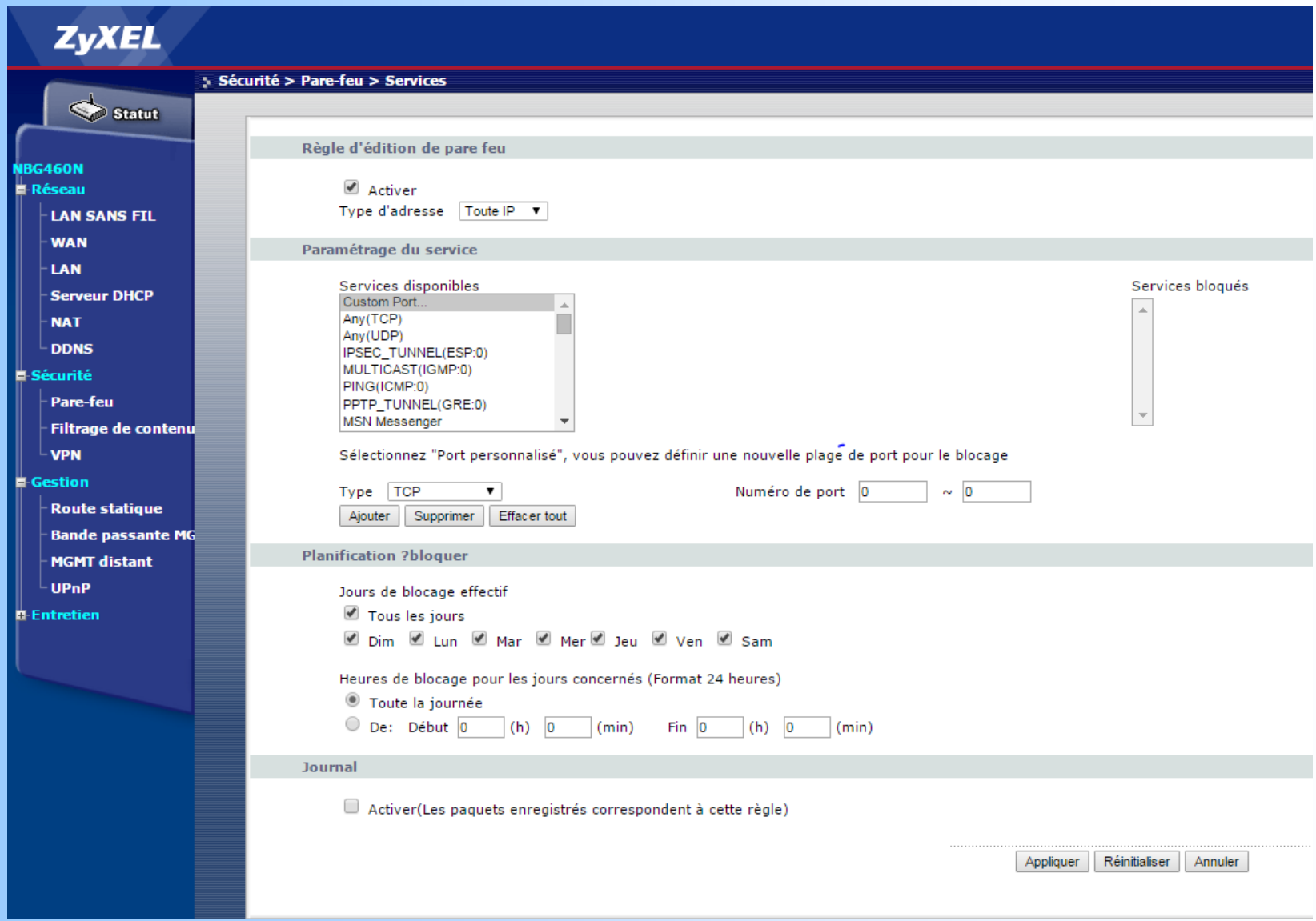



Ajout d'une règle.

ICMP : blocage des «Ping».

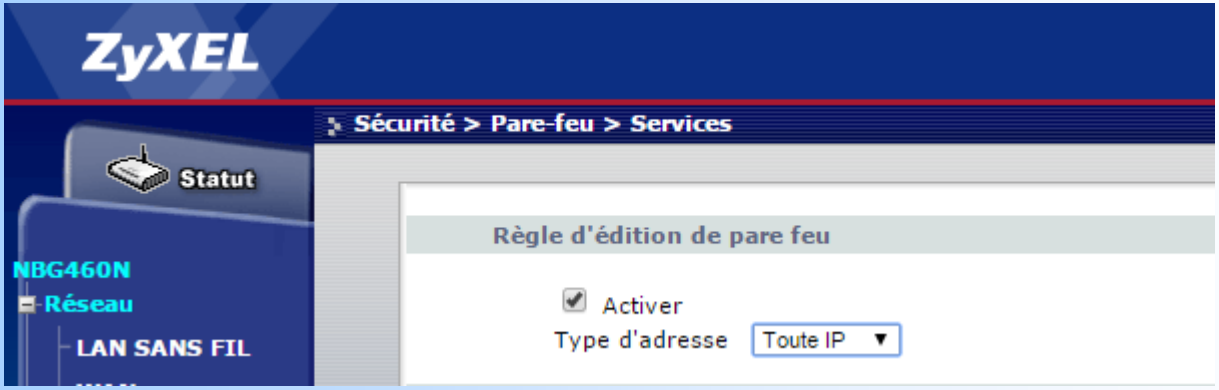
# 6. Utilisation du routeur Zyxel 460N

Après avoir cliquer sur le bouton «Ajouter», on arrive sur ce menu :



# 6. Utilisation du routeur Zyxel 460N

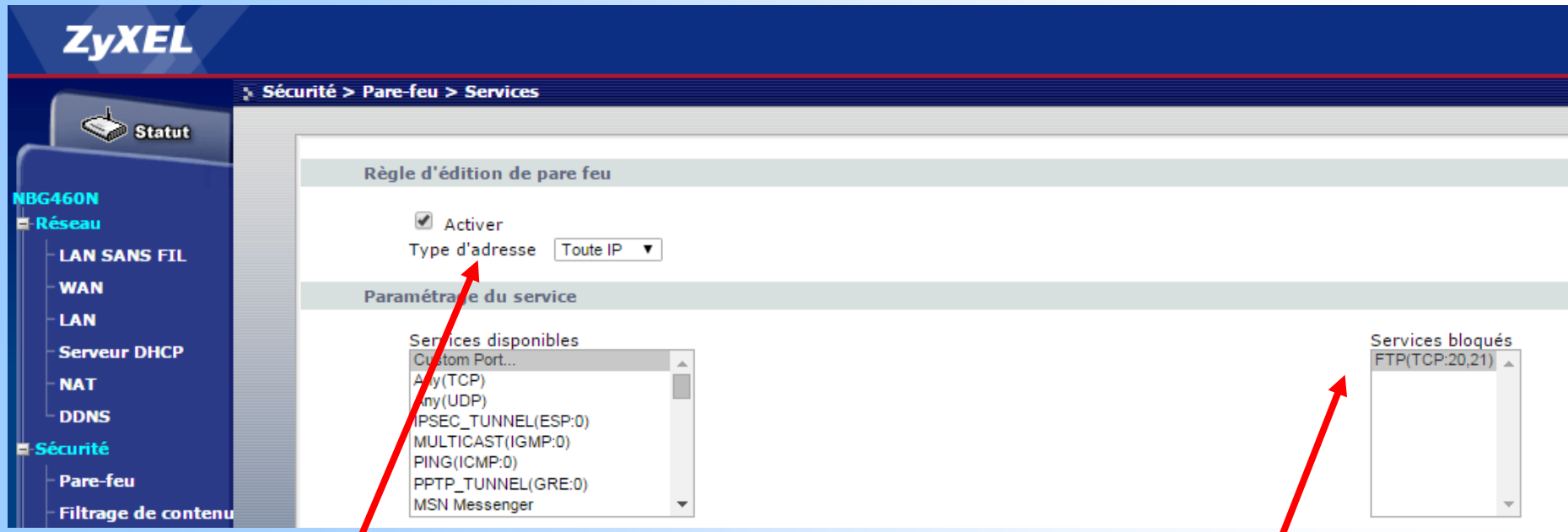
Choix des adresses impliquées à la nouvelle règle :




**Type d'adresse :** on peut appliquer une règle à toutes les adresses, à une pile d'adresses ou à une adresse unique.

# 6. Utilisation du routeur Zyxel 460N

Une liste de services est déjà disponible. Exemple :

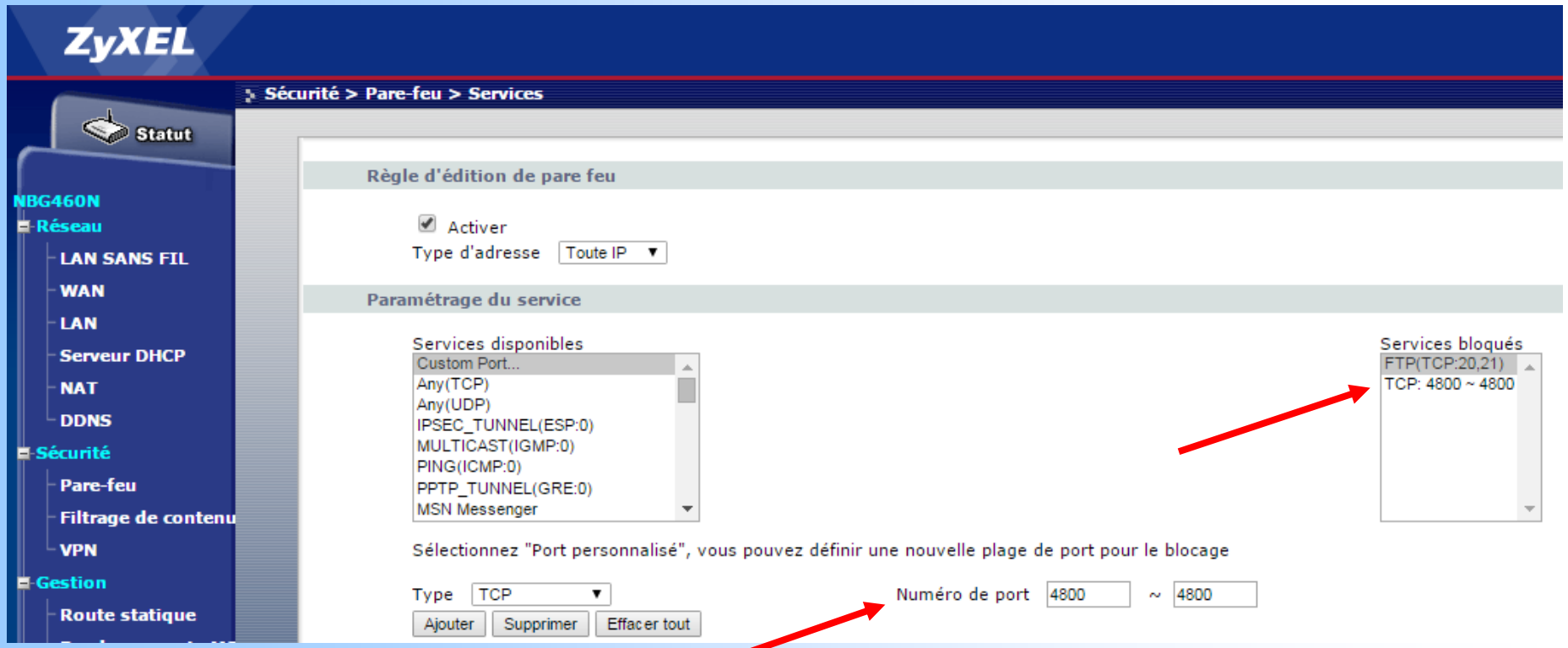



A toutes les adresses IP

Au protocole FTP

# 6. Utilisation du routeur Zyxel 460N

Il est aussi possible d'assigner une règle à un service personnel :




Par exemple le port 4800.

# 6. Utilisation du routeur Zyxel 460N

Et pour finir, il est possible de planifier les jours et les heures d'activation des règles.

Il est aussi possible d'activer le journal.