

03 Le pare-feu

Module 146

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 entêtes 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).

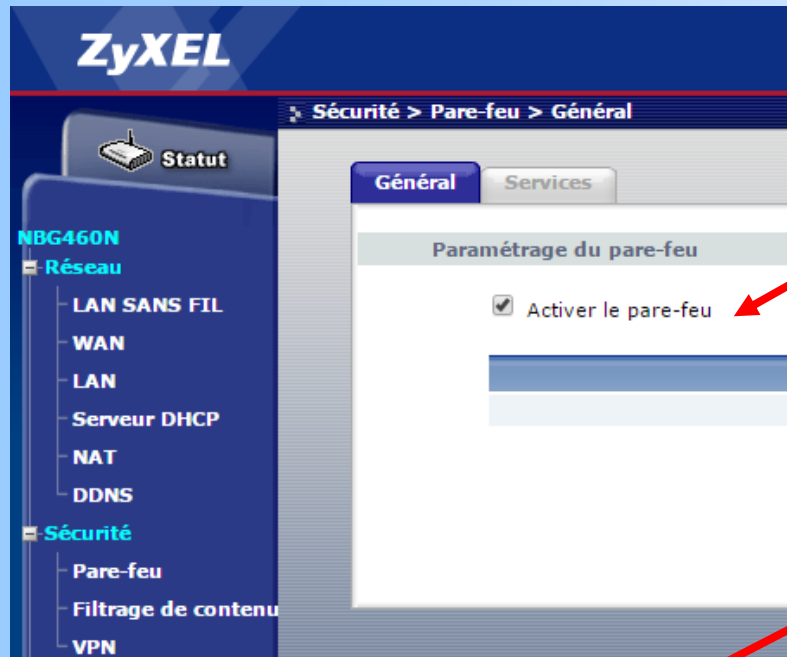
Un firewall effectuant un filtrage applicatif est appelé généralement **passerelle applicative** ou **proxy**.

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

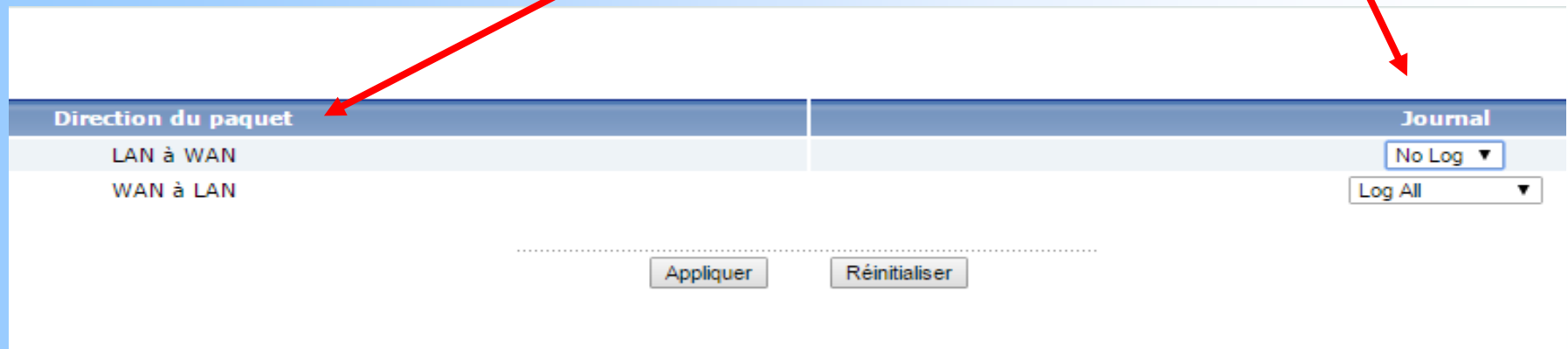
Voyons comment paramétrer le routeur Zyxel :



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 :

ZyXEL

Sécurité > Pare-feu > Général

Statut

NBG460N

Réseau

- LAN SANS FIL
- WAN
- LAN
- Serveur DHCP
- NAT
- DDNS

Sécurité

- Pare-feu
- Filtrage de contenu
- VPN

Gestion

Général Services

ICMP

Répondre aux requêtes Ping sur LAN & WAN ▼

☒ Pas de réponse aux requêtes Ping pour les services non autorisés

Règle de pare feu

#	Activer	Nom du service
---	---------	----------------

Ajouter Nouvelle règle avant la règle 1 (numéro de règle).

Déplacer Règle 1 à la règle 1 (numéro de règle).

Paramètres divers

☒ Ignorer l'itinéraire triangle

Sessions NAT/Pare-feu maxi par utilisateur 4000

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 :

The screenshot displays the ZyXEL NBG460N web interface. The left sidebar shows the navigation menu with categories: Réseau, Sécurité, Gestion, and Entretien. The main content area is titled 'Sécurité > Pare-feu > Services' and shows the 'Règle d'édition de pare feu' configuration page.

Règle d'édition de pare feu

☒ Activer
Type d'adresse: Toute IP

Paramétrage du service

Services disponibles: Custom Port..., Any(TCP), Any(UDP), IPSEC_TUNNEL(ESP:0), MULTICAST(IGMP:0), PING(ICMP:0), PPTP_TUNNEL(GRE:0), MSN Messenger

Services bloqués

Sélectionnez "Port personnalisé", vous pouvez définir une nouvelle plage de port pour le blocage

Type: TCP Numéro de port: 0 ~ 0

Ajouter Supprimer Effacer tout

Planification ?bloquer

Jours de blocage effectif

☒ Tous les jours

☒ Dim ☒ Lun ☒ Mar ☒ Mer ☒ Jeu ☒ Ven ☒ Sam

Heures de blocage pour les jours concernés (Format 24 heures)

☒ Toute la journée

☐ De: Début 0 (h) 0 (min) Fin 0 (h) 0 (min)

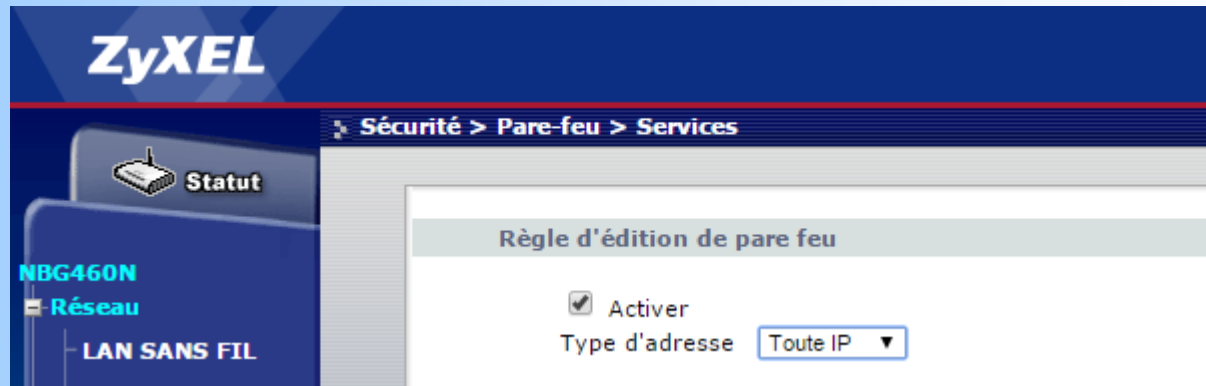
Journal

☐ Activer(Les paquets enregistrés correspondent à cette règle)

Appliquer Réinitialiser Annuler

6. Utilisation du routeur Zyxel 460N

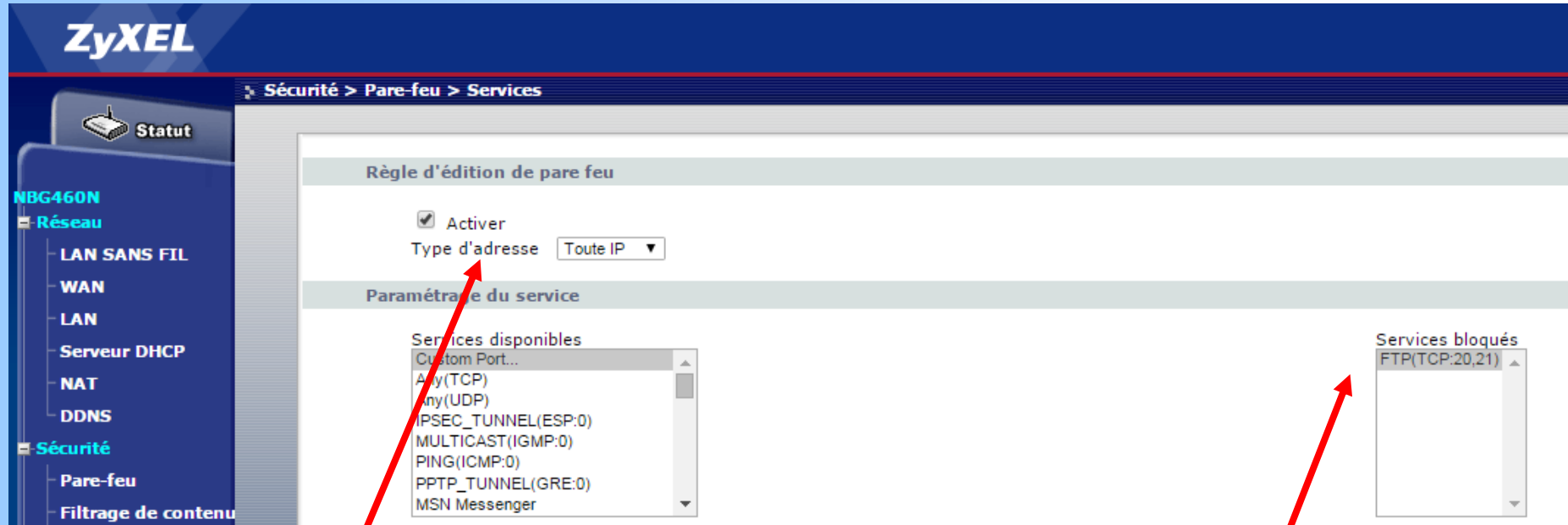
Choix des adresses impliquées à la nouvelle règle :



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 :

The screenshot displays the ZyXEL NBG460N web interface. The left sidebar shows the navigation menu with categories: Réseau (LAN SANS FIL, WAN, LAN), Sécurité (Serveur DHCP, NAT, DDNS, Pare-feu, Filtrage de contenu, VPN), and Gestion (Route statique). The main content area is titled 'Sécurité > Pare-feu > Services' and shows the 'Règle d'édition de pare feu' configuration page. The 'Activer' checkbox is checked, and the 'Type d'adresse' is set to 'Toute IP'. Under 'Paramétrage du service', the 'Services disponibles' list includes 'Custom Port...', 'Any(TCP)', 'Any(UDP)', 'IPSEC_TUNNEL(ESP:0)', 'MULTICAST(IGMP:0)', 'PING(ICMP:0)', 'PPTP_TUNNEL(GRE:0)', and 'MSN Messenger'. A red arrow points from the 'Custom Port...' option to the 'Services bloqués' list on the right. The 'Services bloqués' list contains 'FTP(TCP:20,21)' and 'TCP: 4800 ~ 4800'. Below the service lists, a text prompt says 'Sélectionnez "Port personnalisé", vous pouvez définir une nouvelle plage de port pour le blocage'. The 'Type' is set to 'TCP', and the 'Numéro de port' is configured as '4800 ~ 4800'. A red arrow points from the text 'Par exemple le port 4800.' to the '4800' value in the port range field. At the bottom, there are buttons for 'Ajouter', 'Supprimer', and 'Effacer tout'.

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.

Planification ?bloquer

Jours de blocage effectif

☒ Tous les jours

☒ Dim ☒ Lun ☒ Mar ☒ Mer ☒ Jeu ☒ Ven ☒ Sam

Heures de blocage pour les jours concernés (Format 24 heures)

☒ Toute la journée

☐ De: Début (h) (min) Fin (h) (min)

Journal

☐ Activer(Les paquets enregistrés correspondent à cette règle)

Appliquer

Réinitialiser

Annuler