

03 La DMZ

Zone démilitarisée

Module 146

Introduction

La **DMZ** (**De**Militarized **Z**one) est une zone tampon d'un réseau, située entre le réseau local et le réseau public (Internet).

Elle contient des services publics comme HTTP, SMTP, FTP, DNS, etc...

Son premier but est d'éviter toute connexion directe du réseau interne à Internet.

Son deuxième but est de bloquer toute attaque extérieure depuis le réseau public (Internet).

La gestion de cette zone DMZ peut être gérée par un pare-feu et/ou un serveur proxy.

Politique de sécurité

La politique de sécurité mise en œuvre sur la DMZ est généralement la suivante :

- trafic du réseau externe vers la DMZ autorisé, mais limité par les règles du pare-feu ;
- trafic du réseau externe vers le réseau interne interdit ;
- trafic du réseau interne vers la DMZ autorisé, mais limité par les règles du pare-feu ;
- trafic du réseau interne vers le réseau externe autorisé ;
- trafic de la DMZ vers le réseau interne interdit ;
- trafic de la DMZ vers le réseau externe refusé.

Quelques variantes possibles

La DMZ possède donc un niveau de sécurité intermédiaire, on ne stockera pas des données critiques.

Il est possible d'installer des DMZ en interne afin de cloisonner le réseau interne.

L'inconvénient est que si cet unique pare-feu est compromis, plus rien n'est contrôlé.

Il est cependant possible d'utiliser deux pare-feu en cascade afin d'éliminer ce risque.

Il existe aussi des architectures de DMZ situées entre le réseau Internet et le réseau local, séparée de chaque côté par un pare-feu.

Le schéma ci-dessous représente une architecture DMZ avec un pare-feu à trois interfaces.

Schéma de principe avec pare-feu à trois interfaces

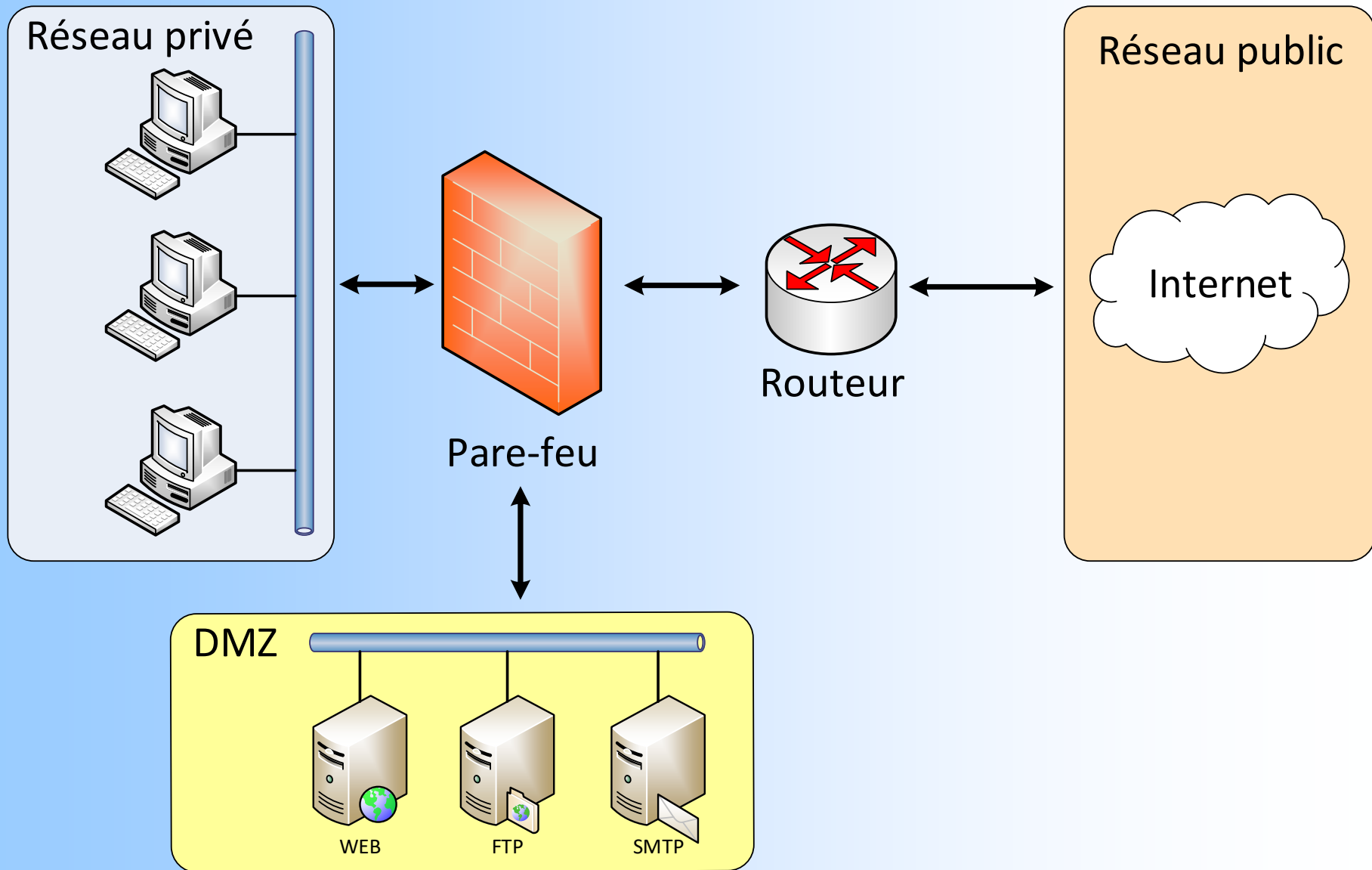


Schéma de principe avec deux pare-feu

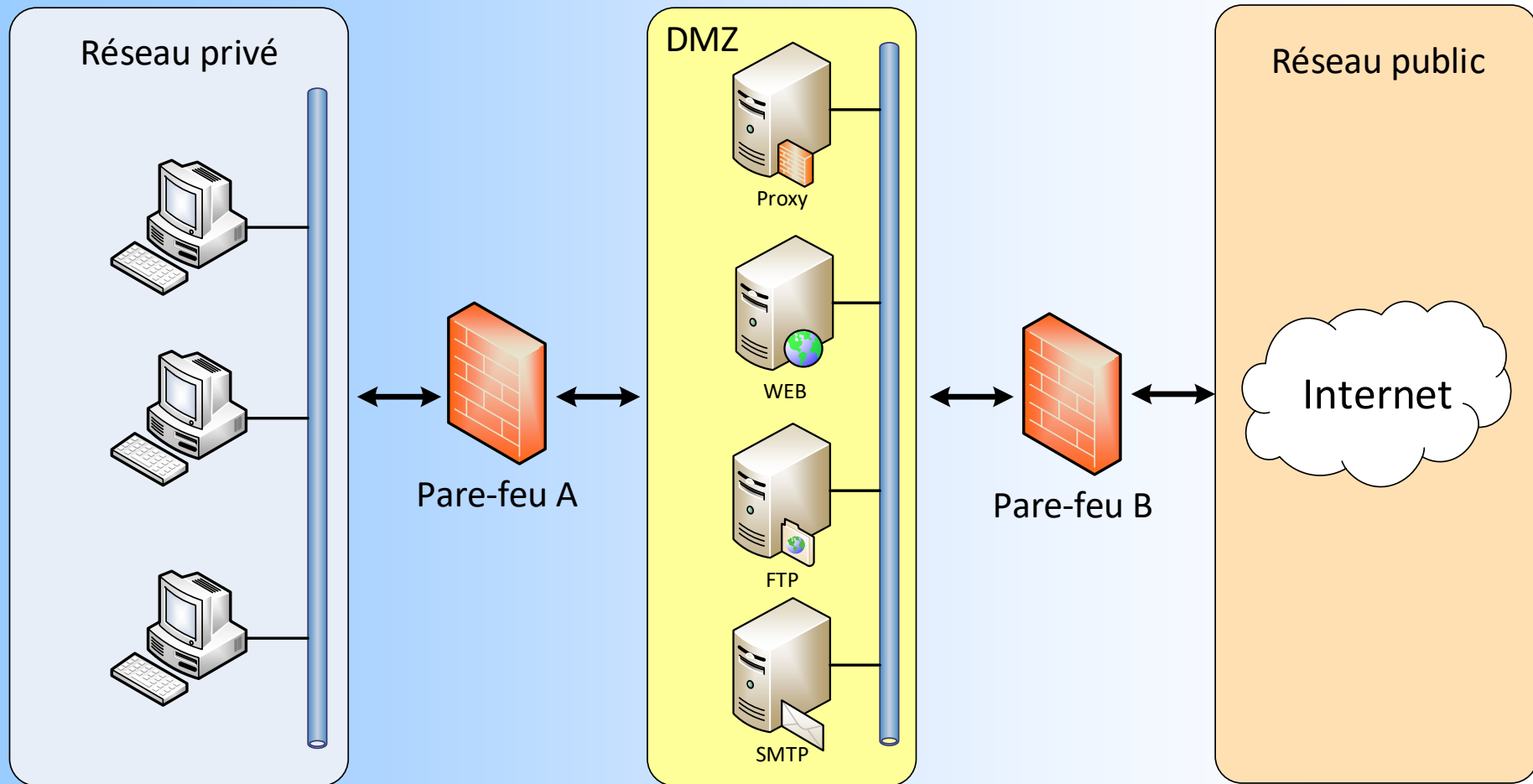
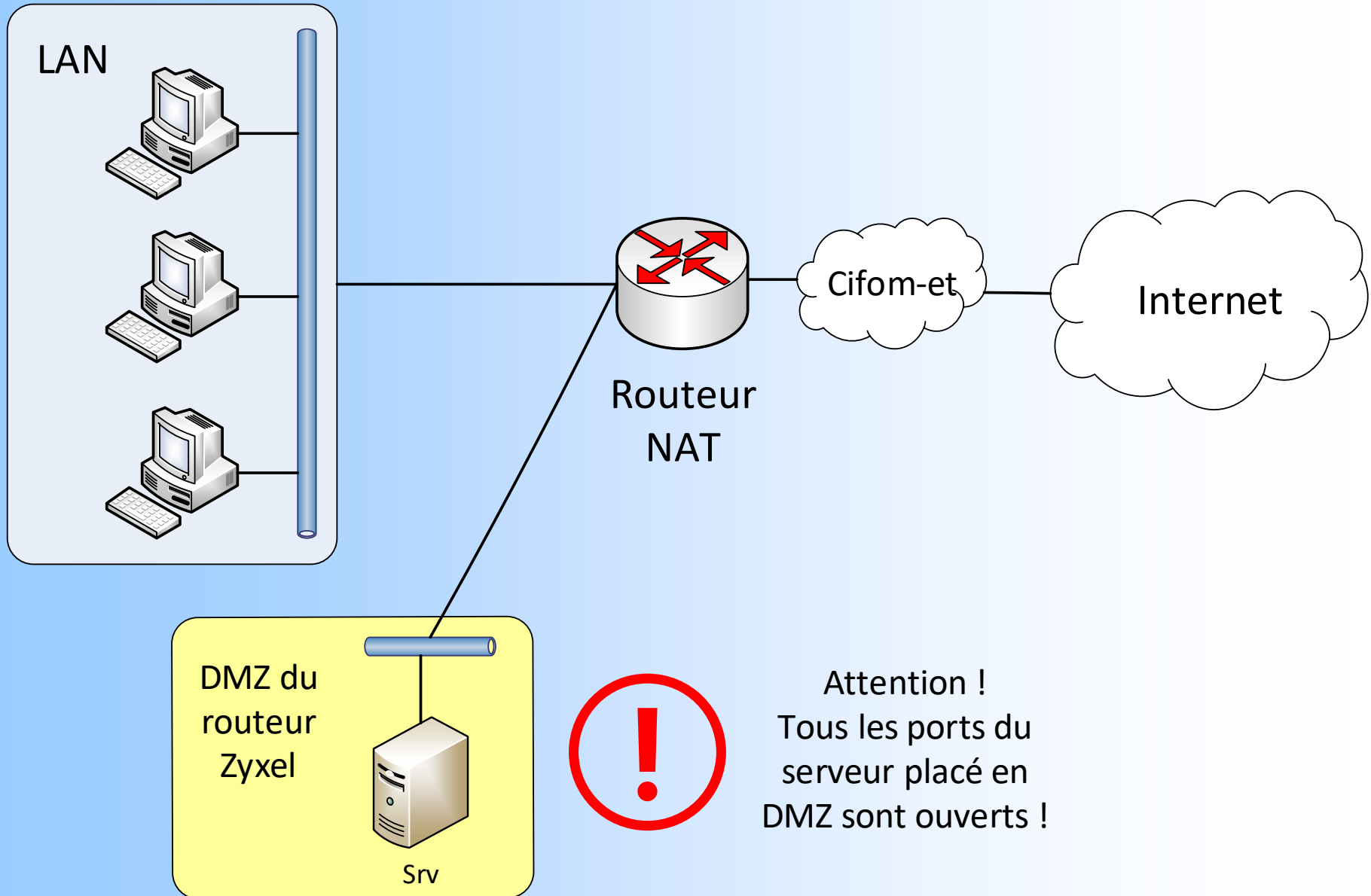


Schéma de principe de la DMZ du routeur Zyxel

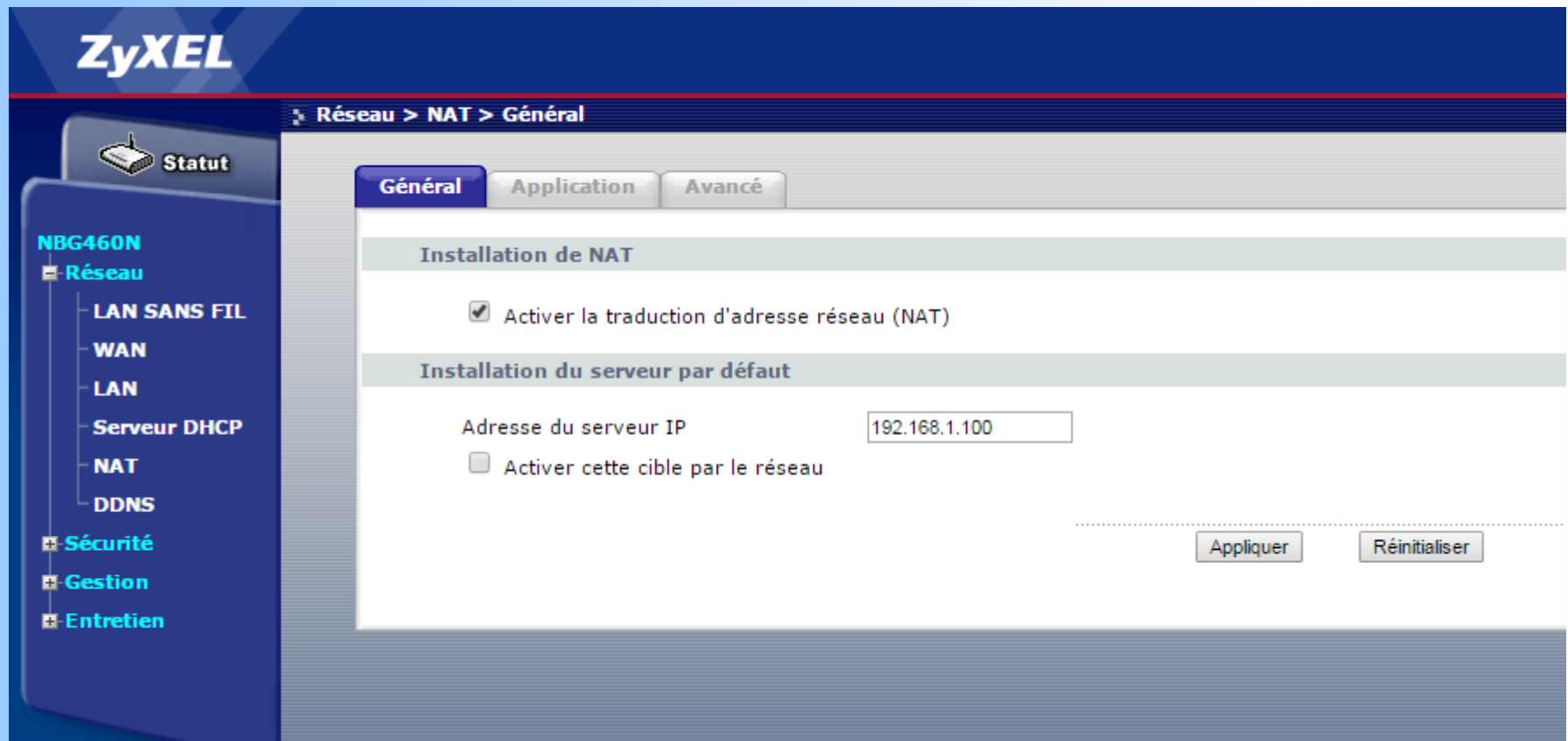


Configuration de la DMZ avec le routeur Zyxel 460N

Pour paramétrer une station du réseau local dans la DMZ, allez dans le menu **Réseau – NAT – Général**.

Entrez l'adresse de la station dans le champs *Adresse du serveur IP* :

Par exemple : 192.168.1.100



The screenshot displays the ZyXEL NBG460N web management interface. The left sidebar shows the navigation menu with 'Réseau' selected. The main content area is titled 'Réseau > NAT > Général'. It features three tabs: 'Général' (selected), 'Application', and 'Avancé'. Under the 'Général' tab, there are two sections: 'Installation de NAT' with a checked checkbox 'Activer la traduction d'adresse réseau (NAT)', and 'Installation du serveur par défaut' with a text input field 'Adresse du serveur IP' containing '192.168.1.100' and an unchecked checkbox 'Activer cette cible par le réseau'. At the bottom right, there are 'Appliquer' and 'Réinitialiser' buttons.

Configuration de la DMZ avec le routeur Zyxel 460N

L'option, *Activer cette cible par le réseau*, correspond au réveil de la station à distance (Wake on line).

