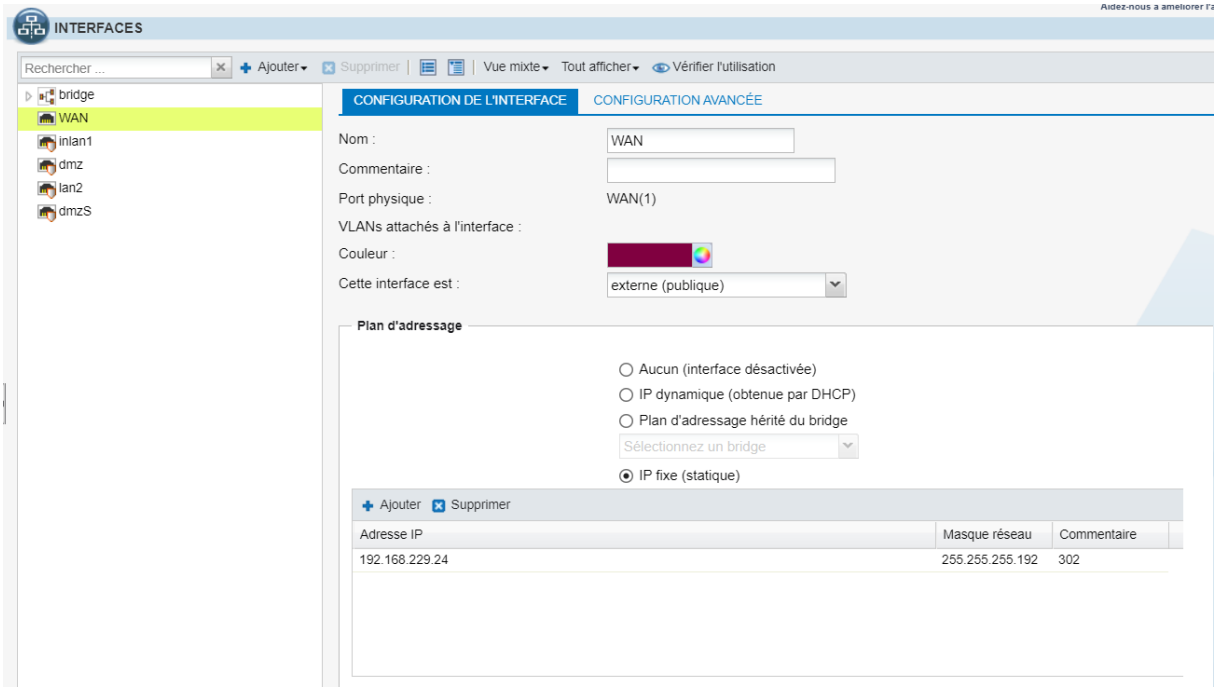
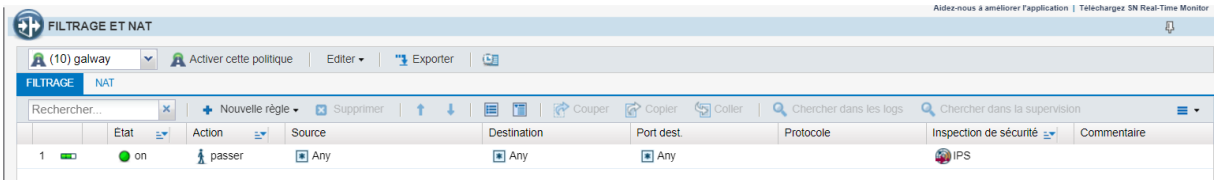
Configuration du Pare-Feu :

On donne accès au pare-feu via internet en donnant un IP fixe au WAN :

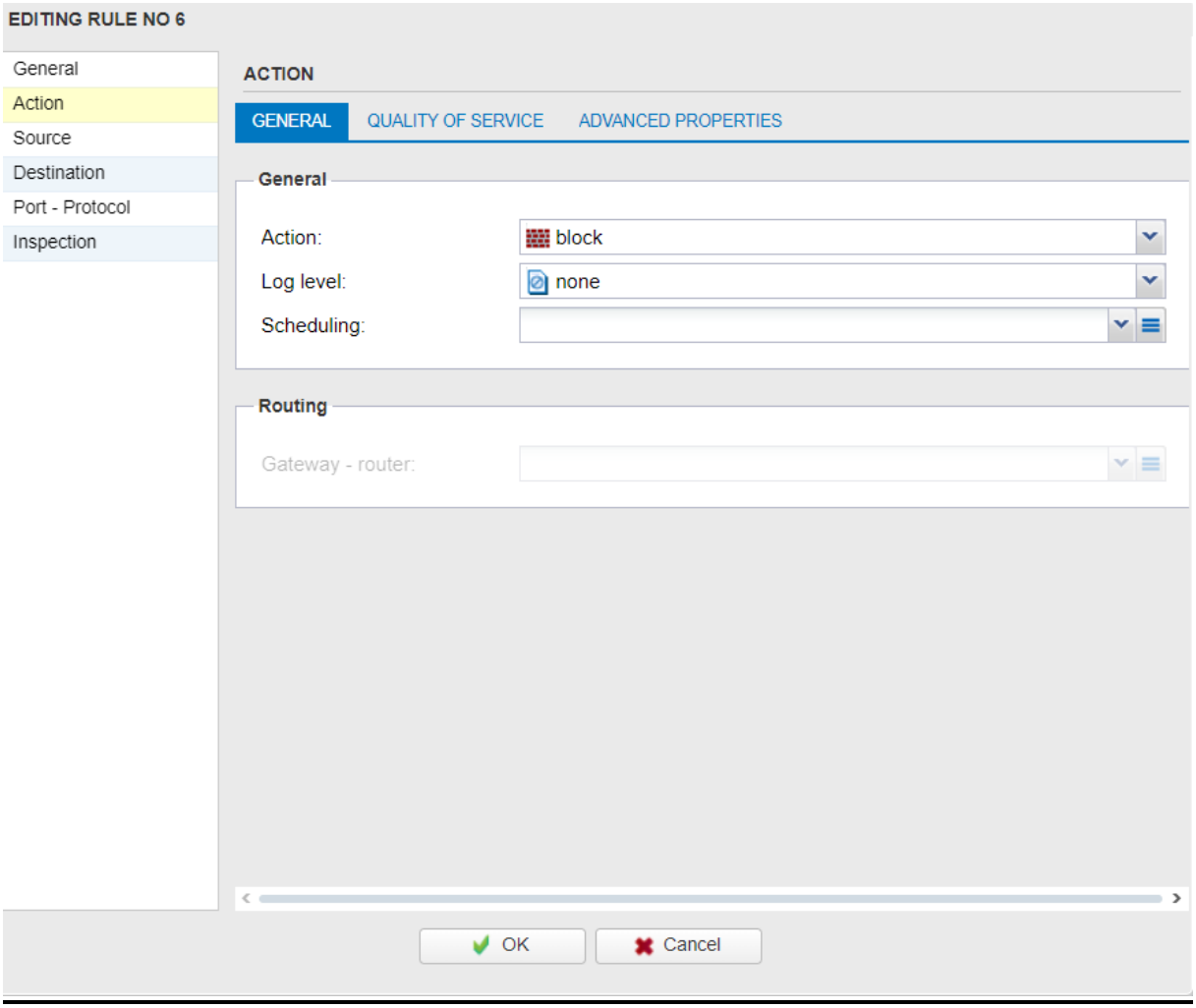


On met le pare-feu en pass all pour avoir accès au pare-feu :



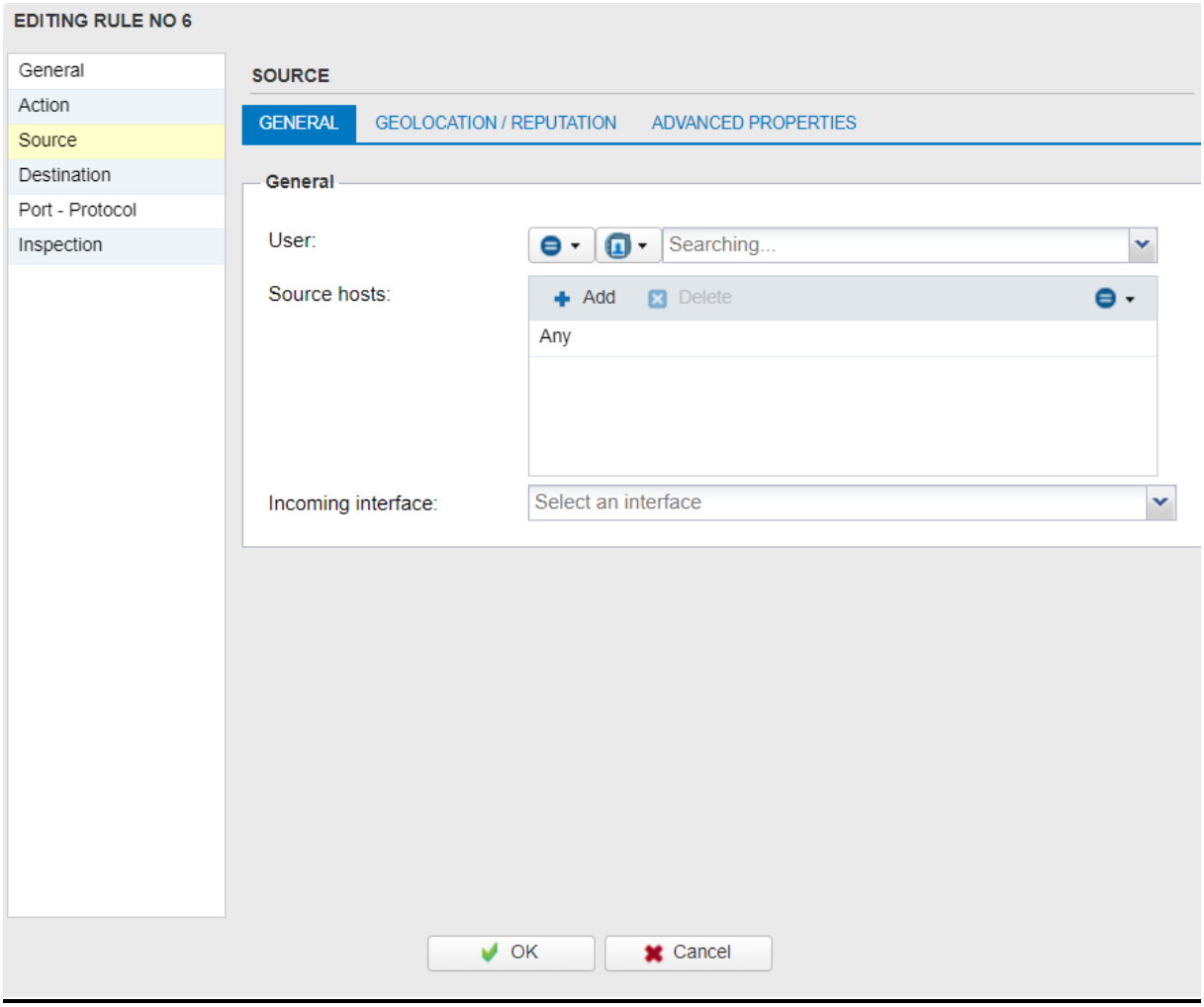
Dans la partie Security Policy - Filtrage et Nat nous créons différentes règles de sécurité de la manière suivante:

Création d'une nouvelle règle simple puis choisir son action



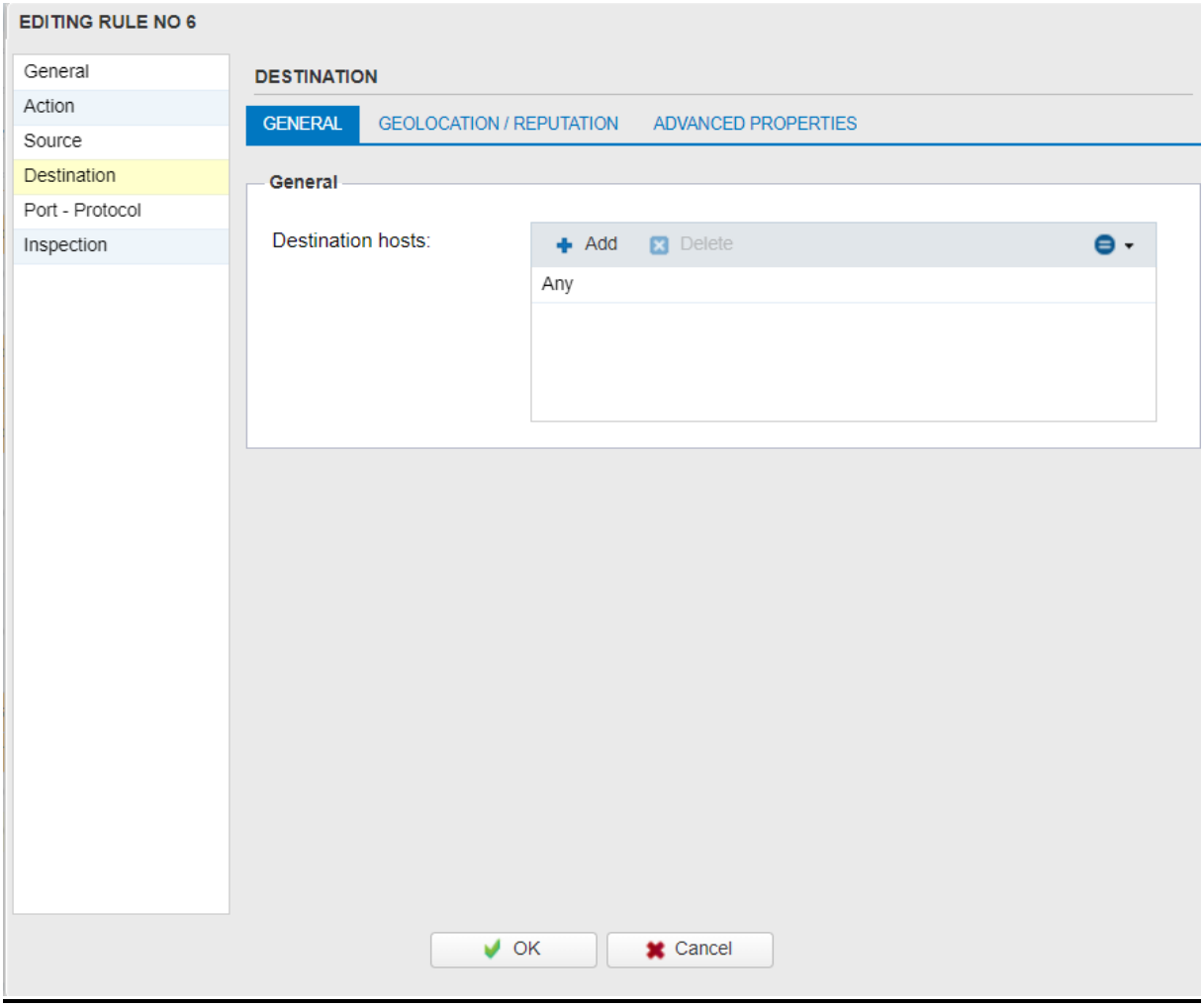
-

Ensuite choisir sa source :



-

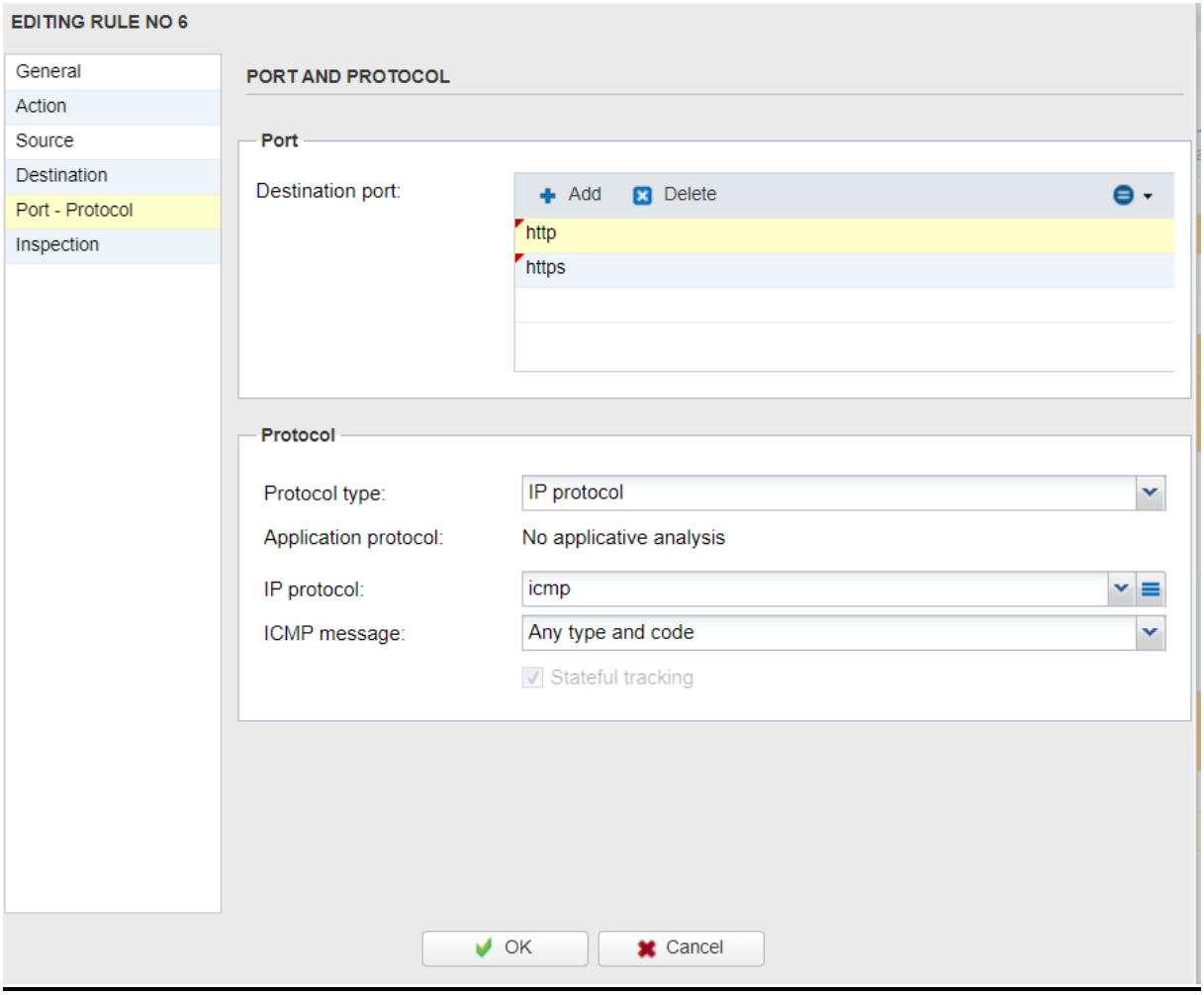
Choisir sa destination :



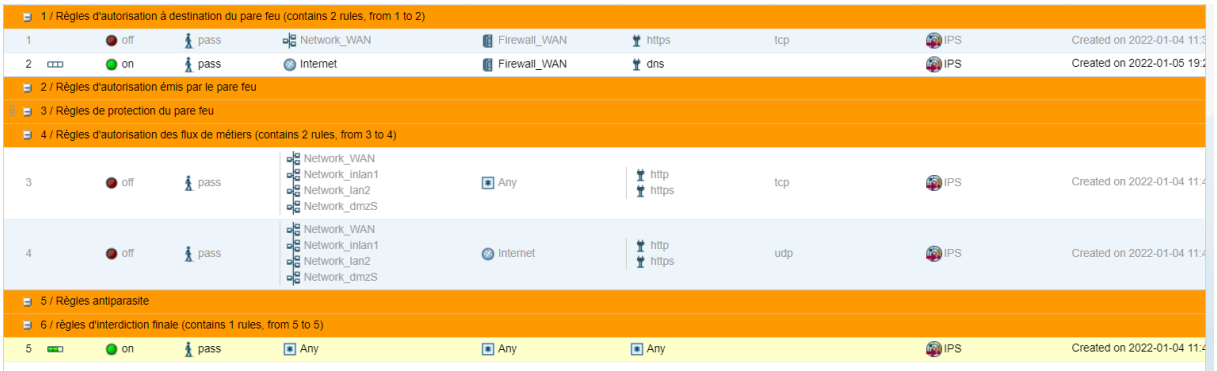
-

-

Choisir son port par exemple ici http/https et son protocole ici ICMP :



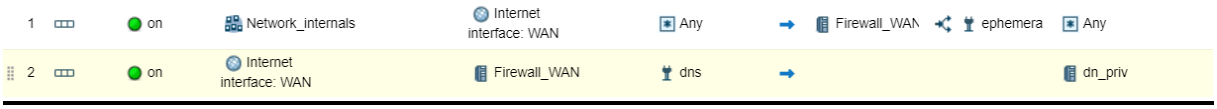
Une fois nos règles crée on les organise selon leurs utilisations :



1. **Permet au réseau WAN à destination du pare feu d'utiliser le port https sur le protocole TCP (inactif)**
2. **Permet à internet d'accéder à la destination du pare feu vers le port du DNS (actif)**

3. **Autorise l’accès pour le réseau WAN, le LAN 1, 2 et la DMZ serveur à n’importe quelle destination via le port http et https par le protocole TCP (inactif)**
4. **Autorise l’accès pour le réseau WAN, le LAN 1, 2 et la DMZ serveur internet via le port http et https par le protocole UDP (inactif)**
5. **Autorise tout (actif)**

Pour le filtrage Nat on crée deux règles :



1. **Les IP provenant d'un réseau interne destiné à Internet, passant par l'interface WAN par n’importe quelle protocol est autorisé à sortir vers l'interface WAN avec un mécanisme appelé "ephemeral ports". Cela signifie que les ports éphémères (temporairement utilisés pour des connexions sortantes) sont utilisés, et NAT est appliqué pour traduire les adresses internes.**
2. **Elle permet aux requêtes DNS externes (venant d’Internet) d’être redirigées vers notre adresse DNS privé (dn_priv),**

Configuration du DHCP :