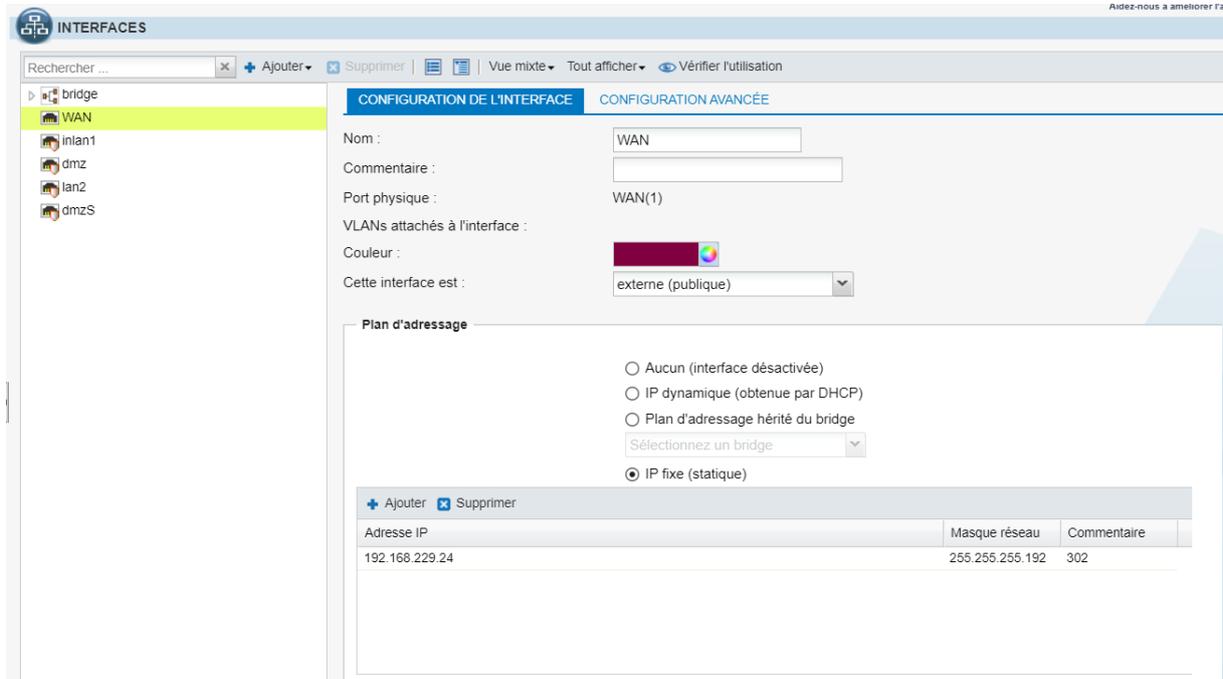
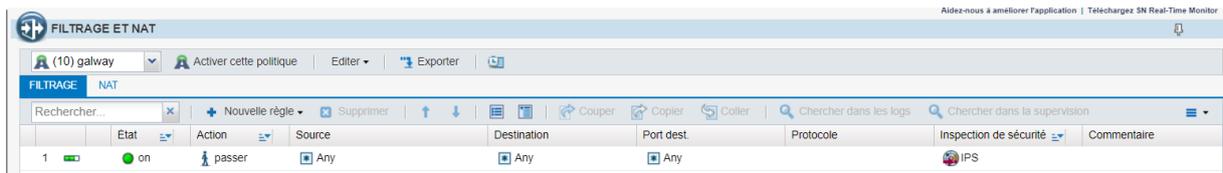


# Configuration du Pare-Feu :

**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**

**EDITING RULE NO 6**

General  
**Action**  
Source  
Destination  
Port - Protocol  
Inspection

**ACTION**

**GENERAL** QUALITY OF SERVICE ADVANCED PROPERTIES

**General**

Action:

Log level:

Scheduling:

**Routing**

Gateway - router:

<  >

-  
**Ensuite choisir sa source :**

EDITING RULE NO 6

General  
Action  
Source  
Destination  
Port - Protocol  
Inspection

**SOURCE**

GENERAL GEOLOCATION / REPUTATION ADVANCED PROPERTIES

**General**

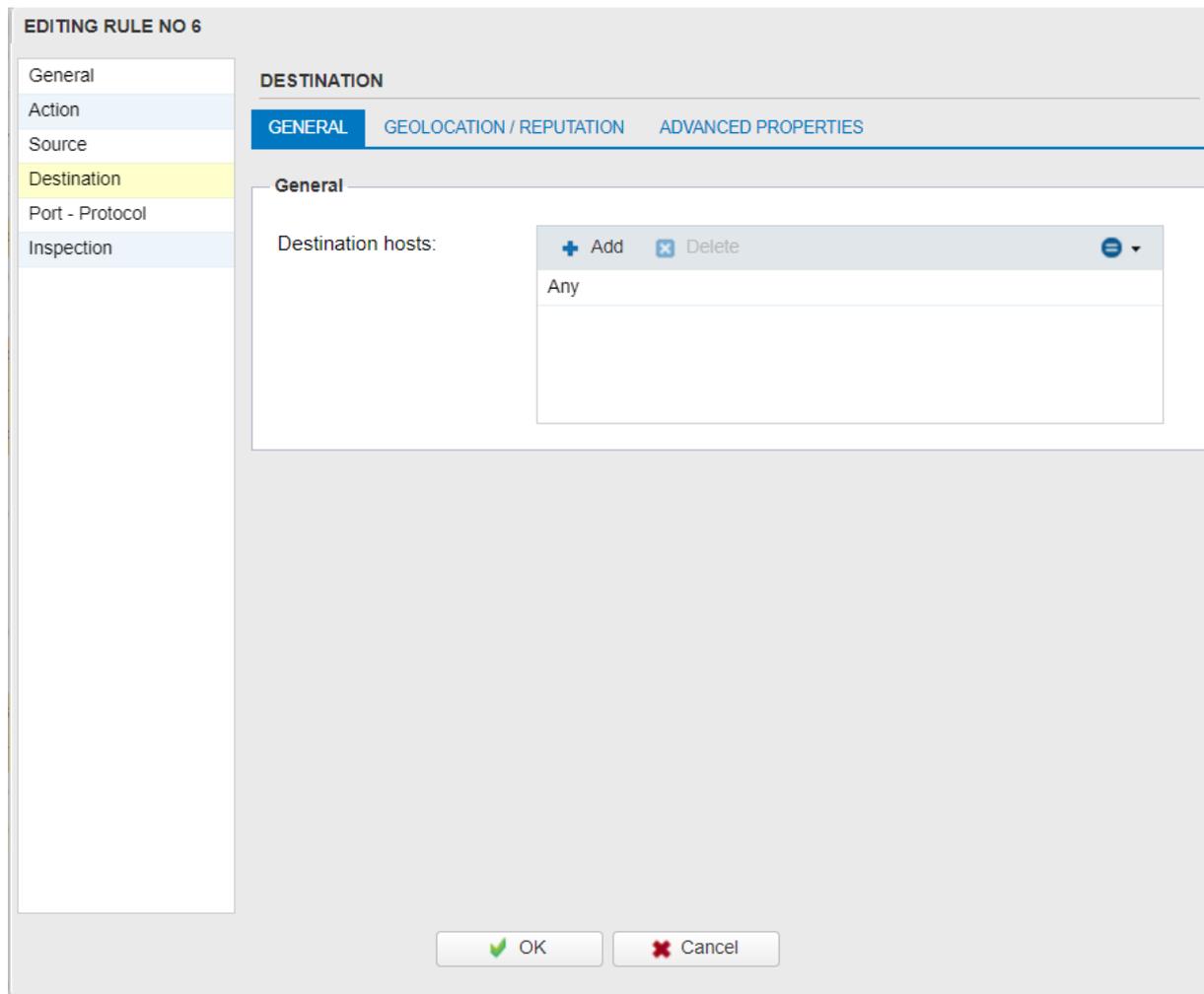
User:

Source hosts:

Incoming interface:

-

**Choisir sa destination :**



-

-

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

**EDITING RULE NO 6**

General  
Action  
Source  
Destination  
**Port - Protocol**  
Inspection

**PORT AND PROTOCOL**

**Port**

Destination port: + Add ✕ Delete

- http
- https

**Protocol**

Protocol type: IP protocol

Application protocol: No applicative analysis

IP protocol: icmp

ICMP message: Any type and code

Stateful tracking

✓ OK ✕ Cancel

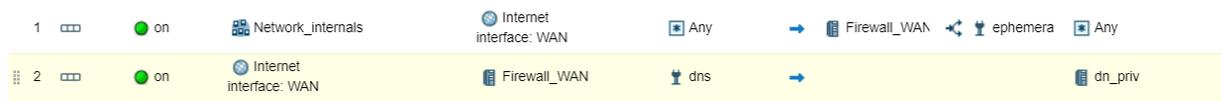
## Une fois nos règles crée on les organise selon leurs utilisations :

1 / Règles d'autorisation à destination du pare feu (contains 2 rules, from 1 to 2)									
1	off	pass	Network_WAN	Firewall_WAN	https	tcp	IPS	Created on 2022-01-04 11:3	
2	on	pass	Internet	Firewall_WAN	dns		IPS	Created on 2022-01-05 19:4	
2 / Règles d'autorisation émis par le pare feu									
3 / Règles de protection du pare feu									
4 / Règles d'autorisation des flux de métiers (contains 2 rules, from 3 to 4)									
3	off	pass	Network_WAN Network_inlan1 Network_lan2 Network_dmzS	Any	http https	tcp	IPS	Created on 2022-01-04 11:4	
4	off	pass	Network_WAN Network_inlan1 Network_lan2 Network_dmzS	Internet	http https	udp	IPS	Created on 2022-01-04 11:4	
5 / Règles antiparasite									
6 / règles d'interdiction finale (contains 1 rules, from 5 to 5)									
5	on	pass	Any	Any	Any		IPS	Created on 2022-01-04 11:4	

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 protocole 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 :**