15/12/2024

Mise en place de Stormshield Virtuel (SNS)

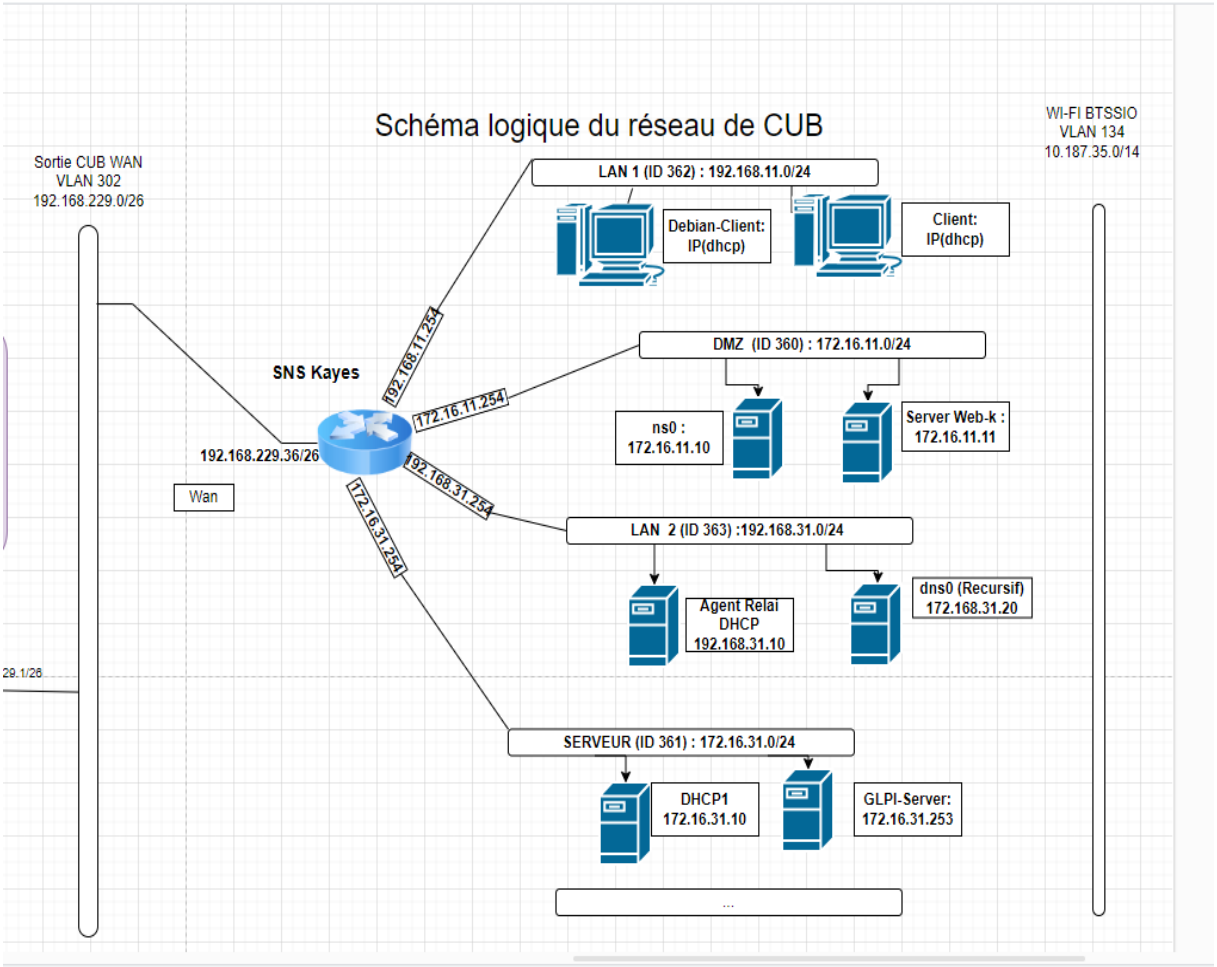
Proxmox

Mamadou CAMARA
[NOM DE LA SOCIETE]

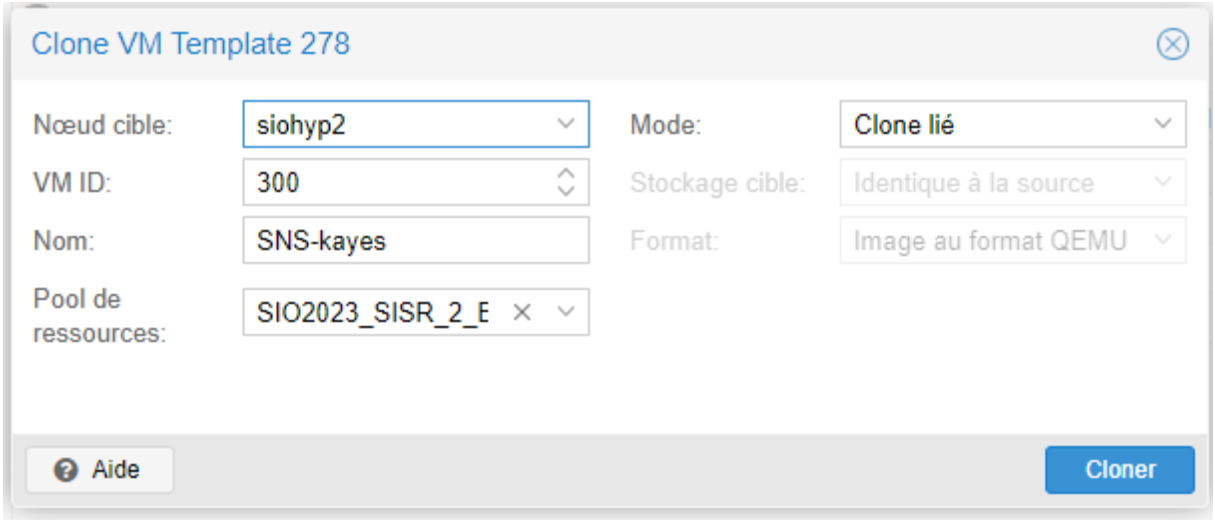
SOMMAIRE

1. Contexte :

Agence	ID VLAN	Adresses de sous-réseaux	Adresses IP de notre firewall Stormshield
Kayes	346	**DMZ :** 172.16.11.0/24	**dmz :** 172.16.11.254
	347	**SERVEURS :** 172.16.31.0/24	**Seveurs:** 172.16.31.254
	348	**LAN 1 :** 192.168.11.0/24	**Lan1 :** 192.168.11.254
	349	**LAN 2 :** 192.168.31.0/24	**Lan2 :** 192.168.31.254
	302	**WAN :** 192.168.229.0/26	**Out :** 192.168.229.36



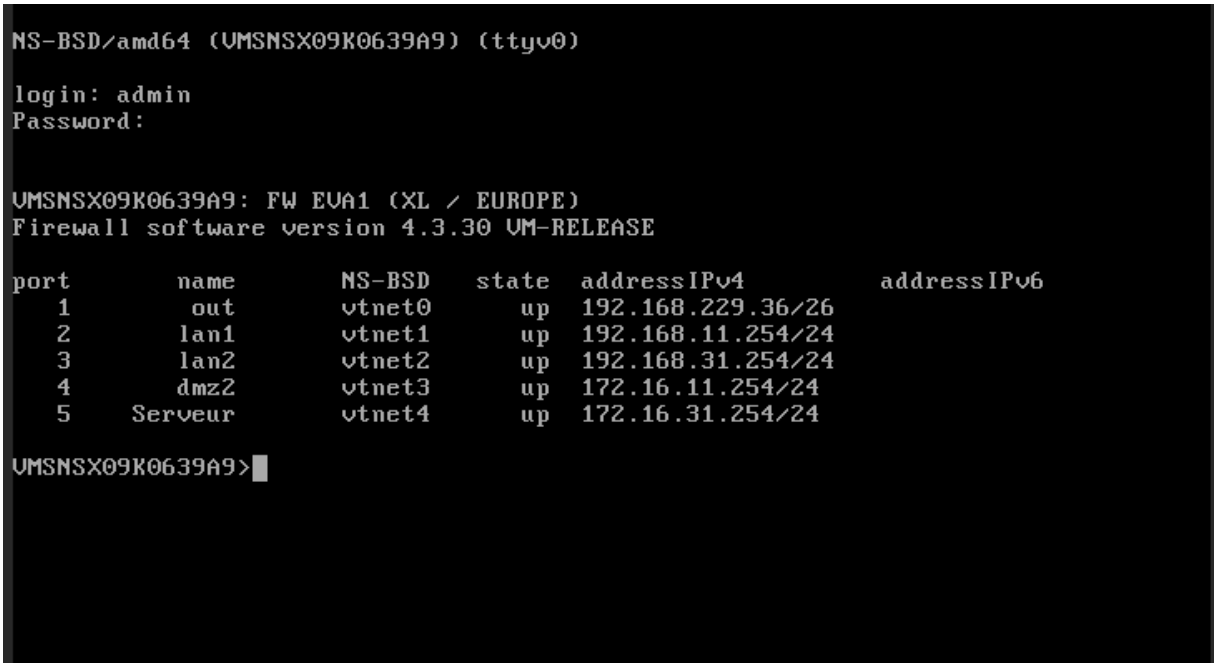
2. Clonage du Template Modele-SNS-4.3 (Clone lié) :



3. Définir les VLAN de chaque interface

Pour définir les VLAN de chaque interface, on click sur le Taplante, on va dans Materiel. Pour l'interface net0 (Out) on met réseau wifi-cub-wan pour pouvoir accéder à l'interface graphique du Stormhield via l'adresse IP obtenue en dhcp lors de l'installation du pare-feu Virtuel.
Sur les autres interfaces, on met nos VLAN internes (LAN1, LAN2, DMZ, Serveur)

4. Démarrer la VM et répondre aux questions de l'assistant



NB : lors de l'installation du pare-feu sur proxmox, on laisse tous les interface en dhcp et on autorise l'accès de Stormshiel depuis l'interface Out.

5. Accéder à l'interface Web du SNS

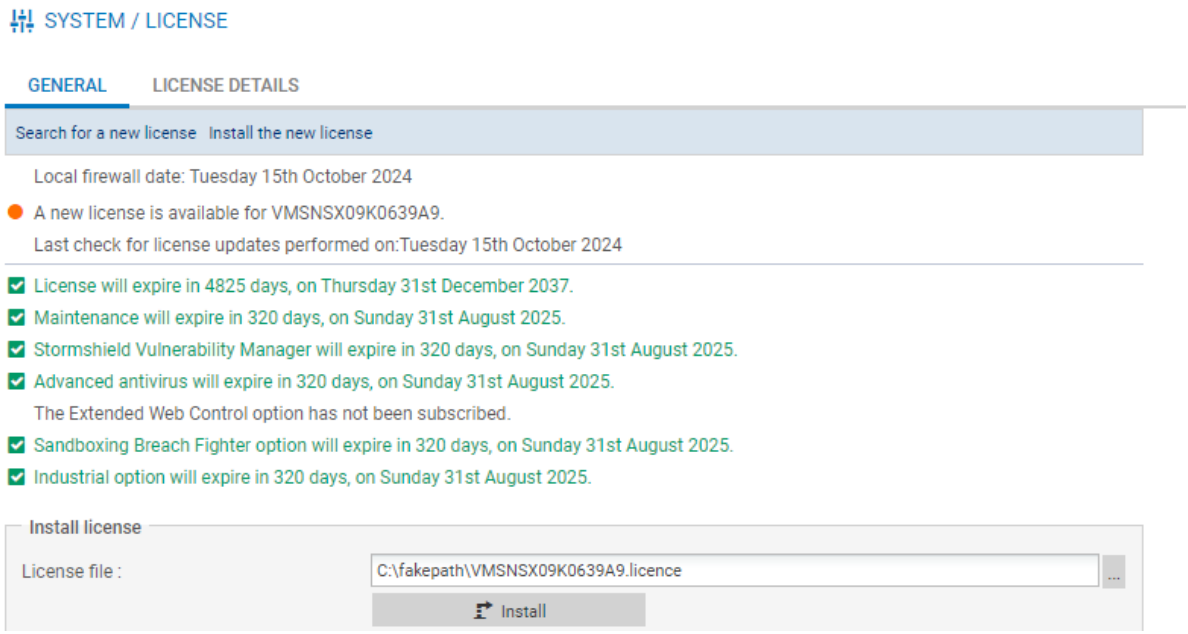
https:// <adresse ip 'Out' en dhcp>

On modifiera ensuite l'adresse IP Out obtenu en DHCP par notre adresse IP publique externe : **192.168.229.36**

6. Activation du SNS

5.1 Mise à jour de la licence

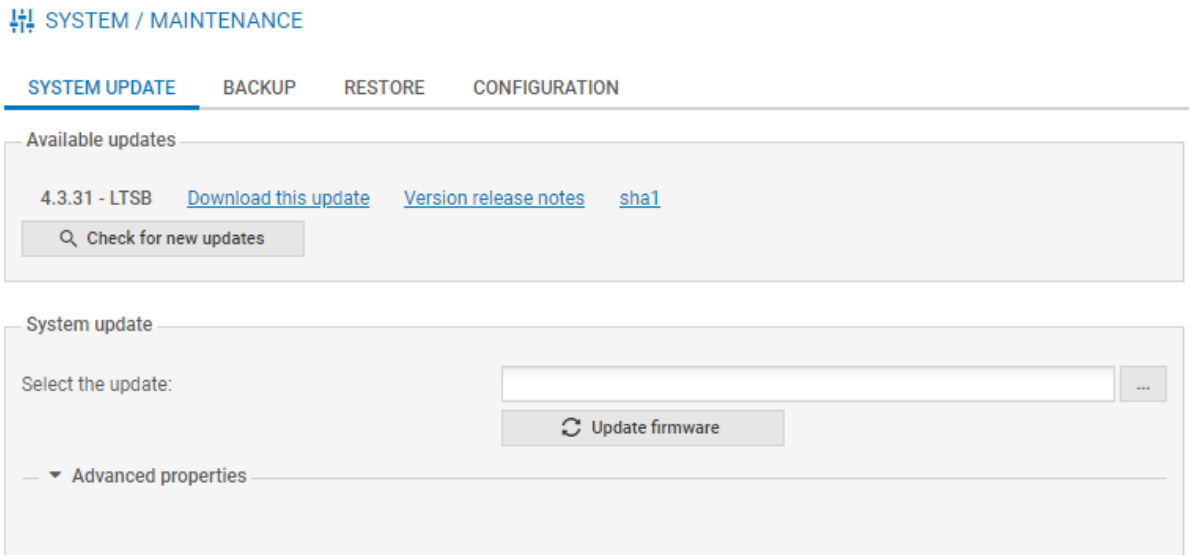
Dans **System/licence**



On choisi le **Fichier : VMSNSX09K0639A9.licence** puis on click sur installer.

5.2 Mise en oeuvre de la HA

Le Kit d'activation/mise à jour est à utiliser pour le déploiement initial d'une nouvelle VM.
Fichier : vminit-VMSNSX09K0639A9.maj



5.3 Mise à jour du Firmware

L'image est en version 4.3.27 LTSB. La mise à jour en version supérieure (4.3.30) peut être réalisée une fois l'installation initiale terminée, via l'interface d'administration du firewall.

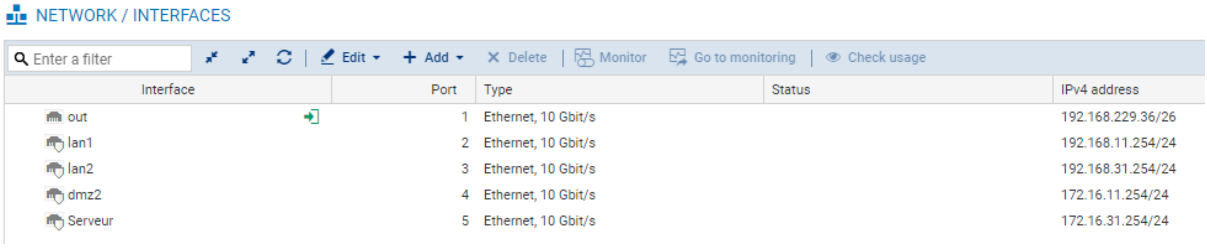
Utiliser le fichier **fwupd-4.3.30-SNS-amd64-XL-VM.maj** dans le menu Systeme > Maintenance

7. Configuration des interfaces réseaux

La première interface du pare-feu est nommée « OUT », la seconde « IN » et les restes des interfaces DMZ.
NB : L'interface OUT est une interface externe que l'on utilise pour pouvoir accéder à internet et le restes des interfaces sont internes.

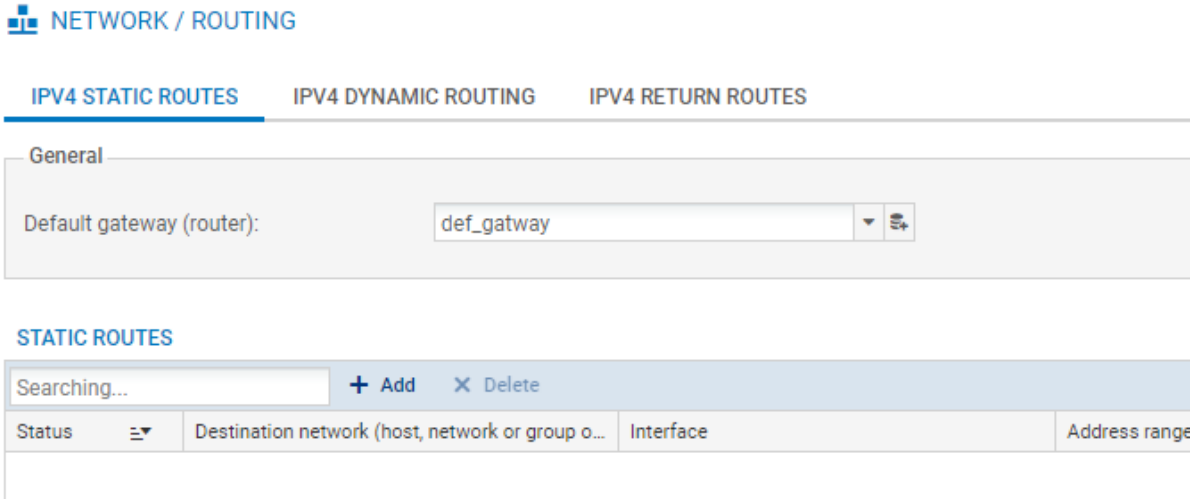
Nous allons procéder à la configuration des inrfaces du pare-feu

La configuration des interfaces s'effectue dans le menu Configuration / Réseau / Interfaces



8. Route par défaut

La configuration de la passerelle par défaut de notre pare-feu SNS doit pointer sur l'adresse IP du parefeu SNS du siège (enseignant) : 192.168.229.1 : Cliquez **Configuration / Réseau / Routage / onglet Routes statiques IPv4**.



On définie l'Objet def_gatway avec l'adresse IP de la passerelle : **192.168.229.1**

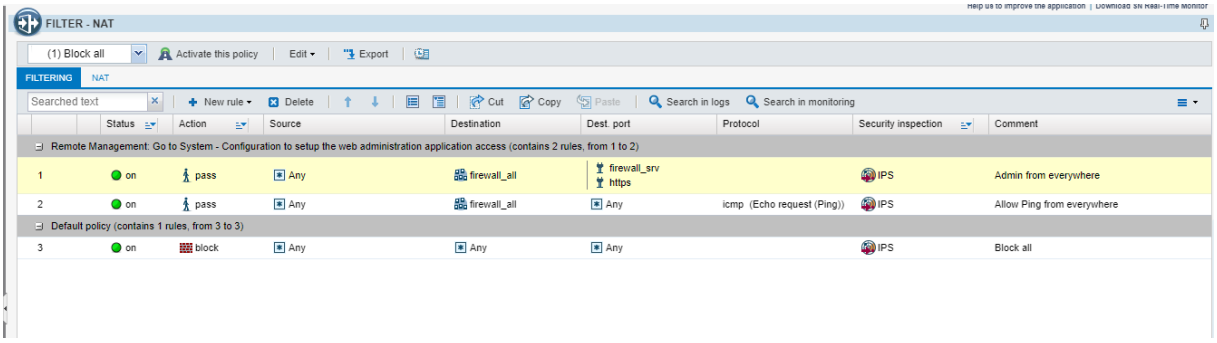
9. Mise en œuvre de la translation d'adresse (Internet)

Ouvrez le menu **Configuration / Politique de sécurité / Filtrage et NAT.**

Vous allez mettre en place une nouvelle politique de sécurité, il faudra commencer par désactiver la règle de filtrage Pass all et ajouter les règles de filtrage qui respecteront le cahier des charges décrit ci-après.

Étape 1 : Copiez la politique de filtrage/NAT (1) Block all vers une autre politique vide où nous allons les copier les règles de NAT.

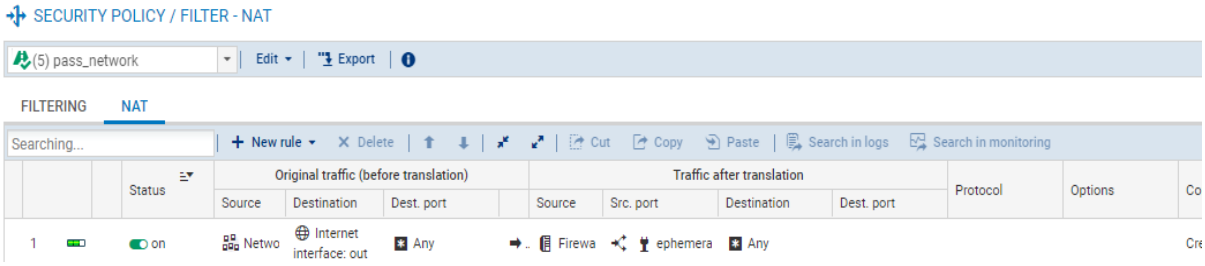
- **Dans la liste déroulante des politiques de sécurité, choisissez (1) Block all.**



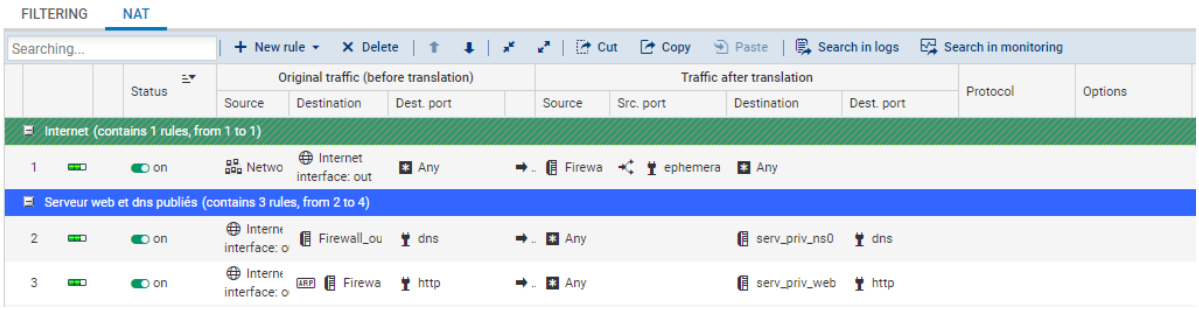
<u>Cliquez Éditer puis copier vers et choisir une politique vide (Filter 05).</u>

- **Cliquez Sauvegarder les modifications…**
- **Dans la liste déroulante des politiques de sécurité, choisissez la politique copiée (05) Block all. Cliquez Éditer puis Renommer et renommez-là en Utilisateurs_Block all & NAT, puis Mettre à jour.**
- **Cliquez sur le bouton Appliquer puis Activer la politique "Utilisateurs_Block all & NAT".**
- **Dans la liste des politiques de sécurité, choisissez la politique précédente, celle où vous avez défini du NAT puis sélectionnez la règle de NAT et cliquez sur Copier.**
- **Dans la liste des politiques de sécurité, choisissez la politique (06) Utilisateurs_Block all & NAT / onglet NAT puis cliquez sur Coller. La règle de NAT/PAT est copiée.**

=> Mise en place de NAT dynamique :



10. Configuration de NAT pour publier le serveur Web interne et DNS autoritaire



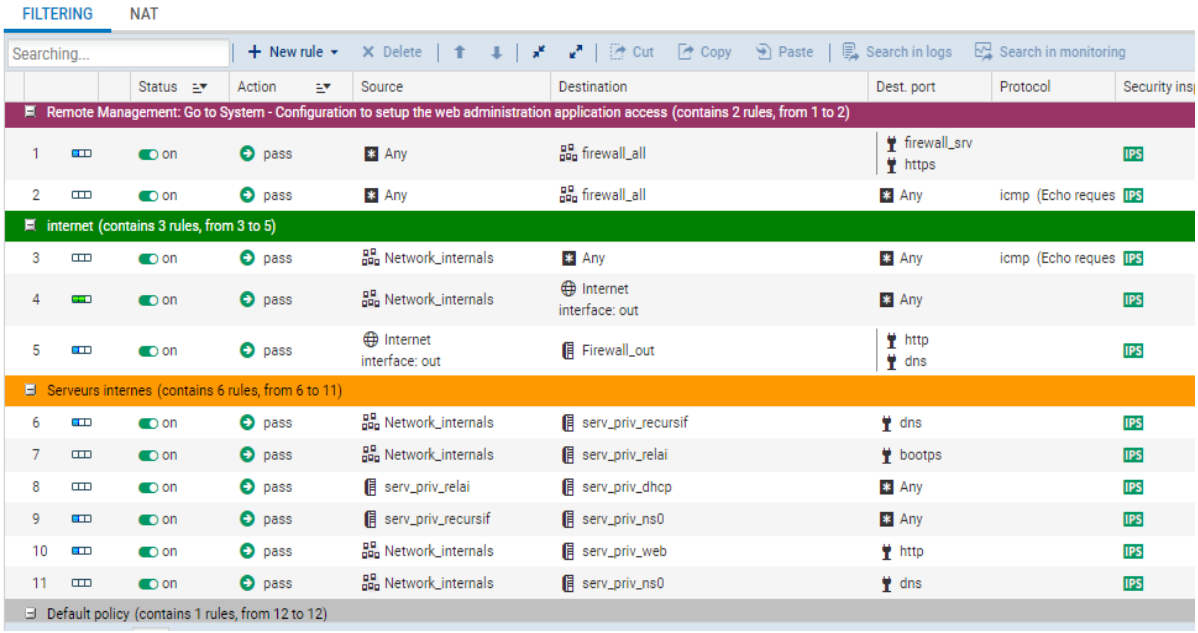
Serveur Web interne

Original trafic	
Source	**internet**
Destination	**Fireware_out (192.168.229.36)**
port	**http (80)**
Après translation	
Source	**any**
destination	**Serveur web privé (172.16.31.253)**
port	**http (80)**

Serveur DNS interne

Original trafic	
Source	**internet**
Destination	**Fireware_out (192.168.229.36)**
port	**dns (53)**
Après translation	
Source	**any**
destination	**Serveur dns privé (172.16.11.10)**
port	**dns (53)**

11. Filtrage pour le contexte



12. Test

```
  GNU nano 7.2                                        db.kayes.cub.fr
;
; BIND data file for local loopback interface
;
$TTL    604800
kayes.cub.fr.           IN      SOA     ns0.kayes.cub.fr. hostmaster.kayes.cub.fr. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL


kayes.cub.fr.   IN      NS      ns0.kayes.cub.fr.
@       IN      A       192.168.229.36
ns0     IN      A       172.16.11.10
www     IN      A       192.168.229.36
glpi    IN      A       172.16.31.253
```

Dans le fichier de configuration de notre serveur dns, on ajoute les informations suivantes :

www IN A 192.168.229.36

pour permettre au réseau externe CUB WAN d'accéder au serveur Web avec le nom **www.kayes.cub.fr**

glpi IN A 172.16.31.253

pour rendre accessible le serveur web depuis interne

NB : 172.16.31.253 est notre serveur web privée

192.168.229.36 est l'adresse IP publique du serveur après translation

```
root@ns0:/etc/bind# dig glpi.kayes.cub.fr

; <<>> DiG 9.18.28-1~deb12u2-Debian <<>> glpi.kayes.cub.fr
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 36969
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;glpi.kayes.cub.fr.             IN      A

;; ANSWER SECTION:
glpi.kayes.cub.fr.      79203   IN      A       172.16.31.253

;; Query time: 8 msec
;; SERVER: 192.168.31.20#53(192.168.31.20) (UDP)
;; WHEN: Tue Oct 15 08:46:37 UTC 2024
;; MSG SIZE  rcvd: 62
```

```
;; WHEN: Tue Oct 15 08:46:37 UTC 2024
;; MSG SIZE  rcvd: 62

root@ns0:/etc/bind# dig www.kayes.cub.fr

; <<>> DiG 9.18.28-1~deb12u2-Debian <<>> www.kayes.cub.fr
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 51232
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;www.kayes.cub.fr.              IN      A

;; ANSWER SECTION:
www.kayes.cub.fr.       79128   IN      A       192.168.229.36

;; Query time: 0 msec
;; SERVER: 192.168.31.20#53(192.168.31.20) (UDP)
;; WHEN: Tue Oct 15 08:47:07 UTC 2024
;; MSG SIZE  rcvd: 61
```