Stormshield

Tutoriels stormshield français

- Règles de base
  - Filtrage de base
  - NAT
- Port-Forwarding Stormshield (redirection de port)
- Générer un certificat SSL/TLS Stormshield depuis un AD CS

Règles de base

Règles de base Stormshield

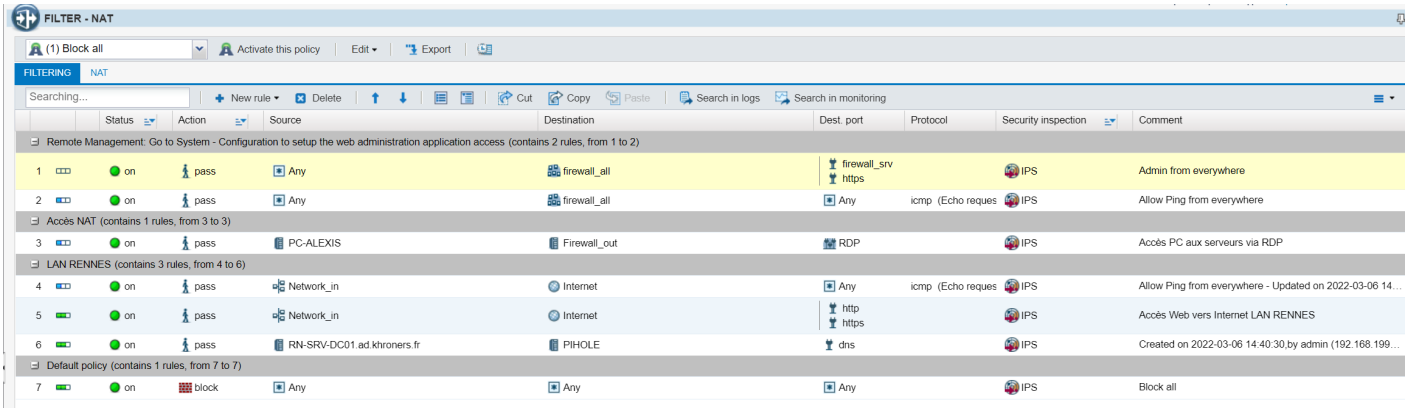
Filtrage de base

Il existe par défaut de nombreux profils disponibles. Le premier est le "(1) Block all". Ce profil est standard : on bloque tout.

On va donc autoriser certains trafics avant la règle qui va tout bloquer.

> Les règles de filtrage s'appliquent de haut en bas.

Par défaut, on a une règle tout en haut qui va nous permettre d'accéder à l'interface d'administration de notre Stormshield.



Pour avoir un fonctionnement "normal" dès le départ, on créer les règles 3 et 4 qui vont nous permettre la résolution DNS et le flux web HTTP / HTTPS.

Règle 3

Cette règle autorise l'accès de mon PC (de mon LAN) vers les serveurs de mon Lab situés dans le LAN du Stormshield.

Règle 4

Cette règle autorise le ping du LAN vers Internet (uniquement)

Règle 5

Cette règle autorise le flux web HTTP / HTTPS du LAN de mon lab vers l'extérieur.

Règle 6

Cette règle autorise le flux DNS de mon Pi-Hole sur mon LAN vers mes deux serveurs contrôleurs de domaine de mon lab.

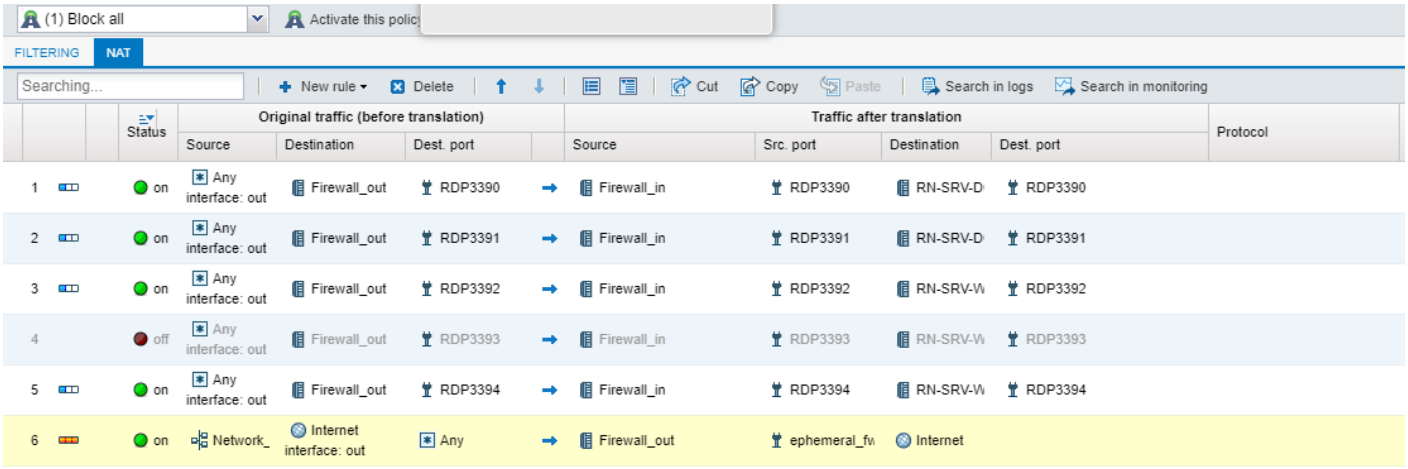
Règle 7

Cette règle bloque le reste du trafic.

NAT

Par défaut, nous n'avons pas de NAT. Cependant, cela est nécessaire.

Une seule règle nous intéresse ici afin d'avoir du NAT fonctionnel pour le LAN : la règle 6.

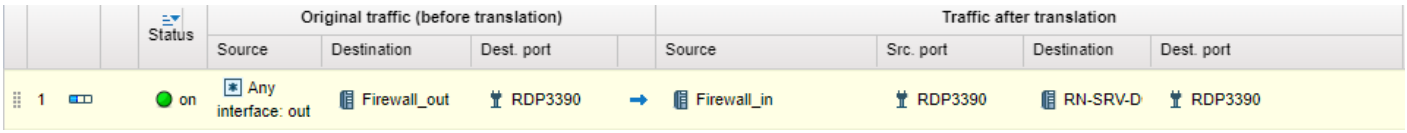


Tout le trafic du LAN vers Internet sera translaté.

Port-Forwarding Stormshield (redirection de port)

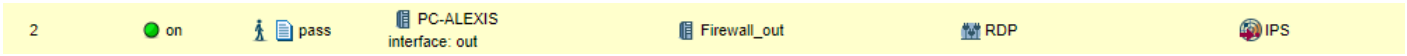
Pour faire passer un port depuis l'extérieur vers une machine du LAN, il faut faire du **port-forwarding** (ou **redirection de port**)

Sous "**Configuration**", "**Filter - NAT**" et l'onglet "**NAT**", on ajoute une règle semblable à celle-ci :



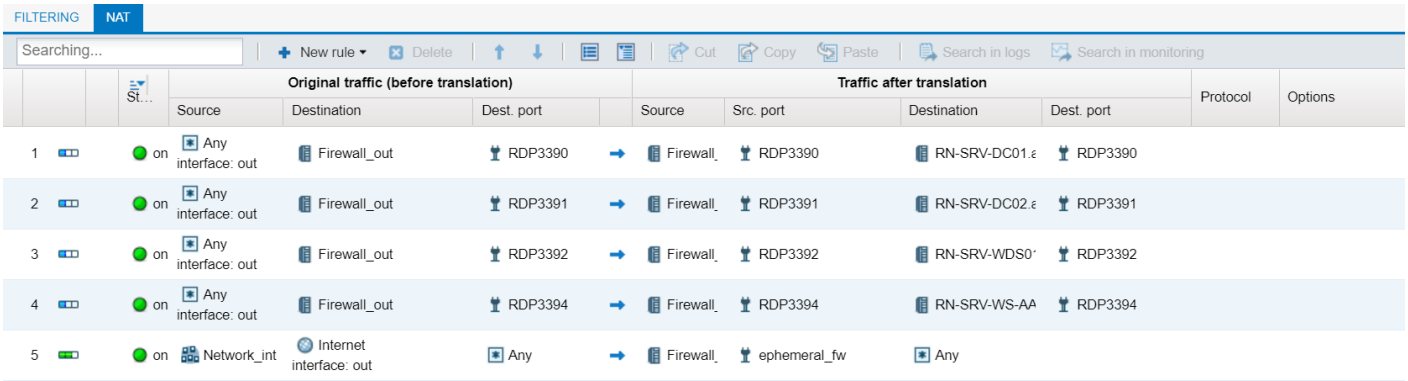
Ici, le trafic arrivant sur l'interface **WAN** du Stormshield avec le port **3390** est redirigé vers **RN-SRV-DC01** avec le port **3390**.

Il faut ensuite autoriser ce trafic dans l'onglet "**Filtering**" :



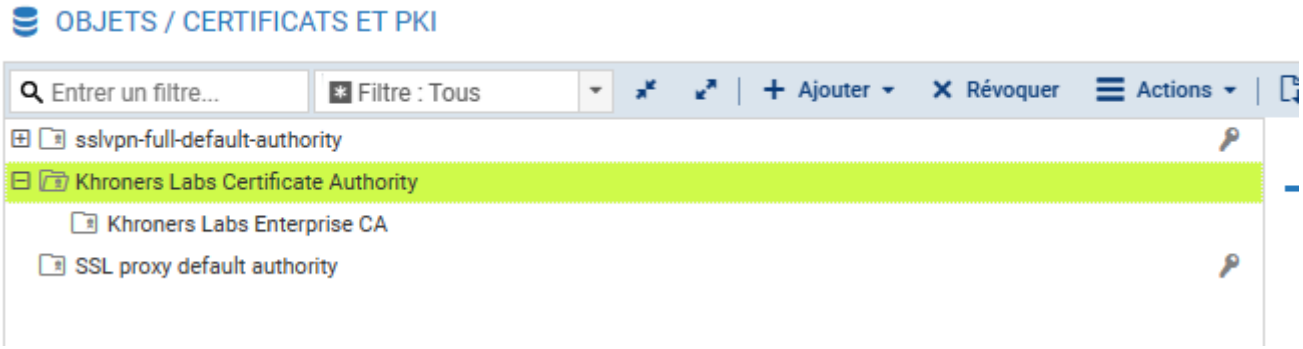
> Pensez à remplacer "**RDP**" par le port que vous avez mis à la première étape. Dans mon cas, j'ai 4 règles de redirection de ports (**3390** à **3394**). Donc "**RDP**" est un groupe de ports.

Dans mon cas :



Générer un certificat SSL/TLS Stormshield depuis un AD CS

On ajoute nos certificats de l'autorité de certification racine et de l'autorité de certification intermédiaire.

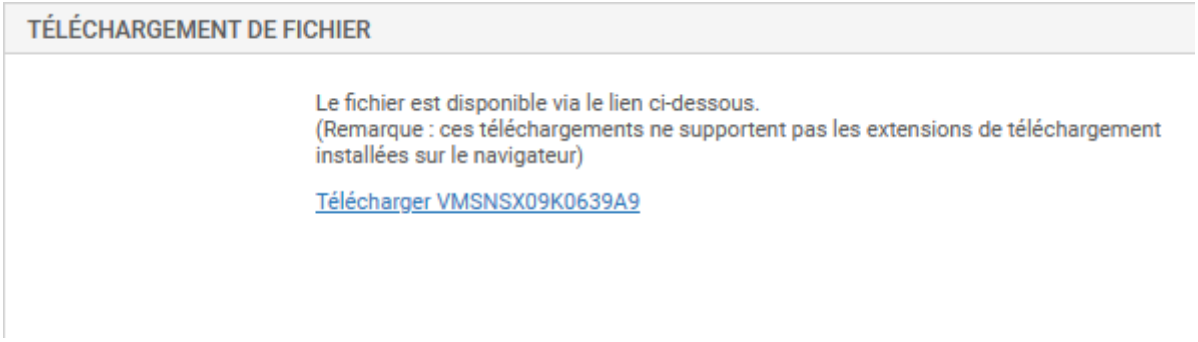


En CLI, on demande un certificat :

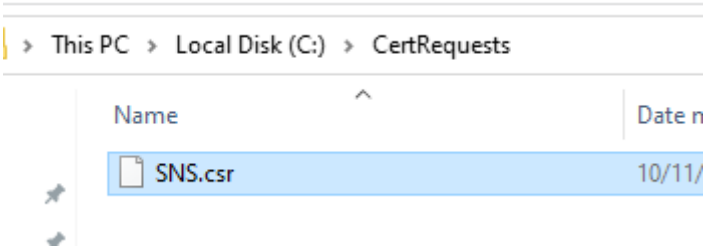
```
PKI REQUEST CREATE type=server cn=stormshield.home.khroners.fr C=FR ST=Bretagne L=Rennes
O="Khroners Labs" OU=IT shortname=sns.home.khroners.fr-20231110 size=4096
ALTNAMES=stormshield.home.khroners.fr
```

On récupère la demande :

```
PKI REQUEST GET name=sns.home.khroners.fr-20231110 format=pem
```



On place notre fichier dans un dossier que l'on renomme "SNS.csr".



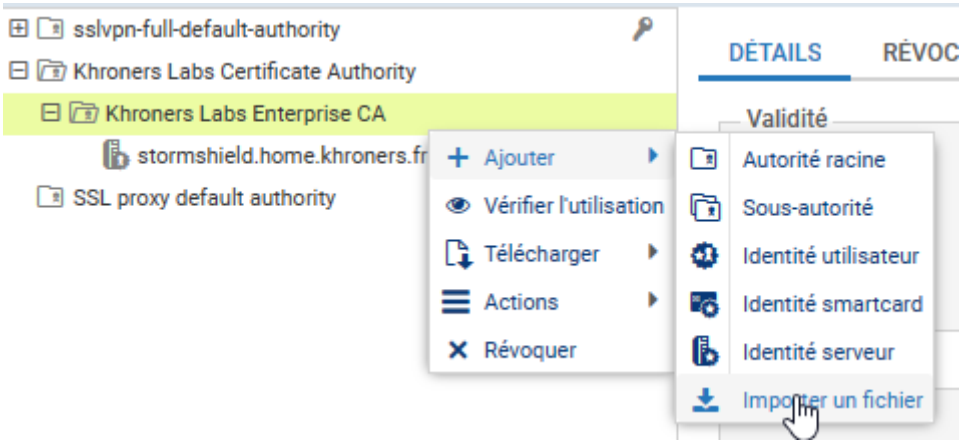
Dans AD CS, on crée notre modèle comme ici : [Creating a Microsoft Certificate Authority Template for SSL certificate creation in vSphere 6.x/7.x (2112009)].

On en profite pour passer le chiffrement en 4096.

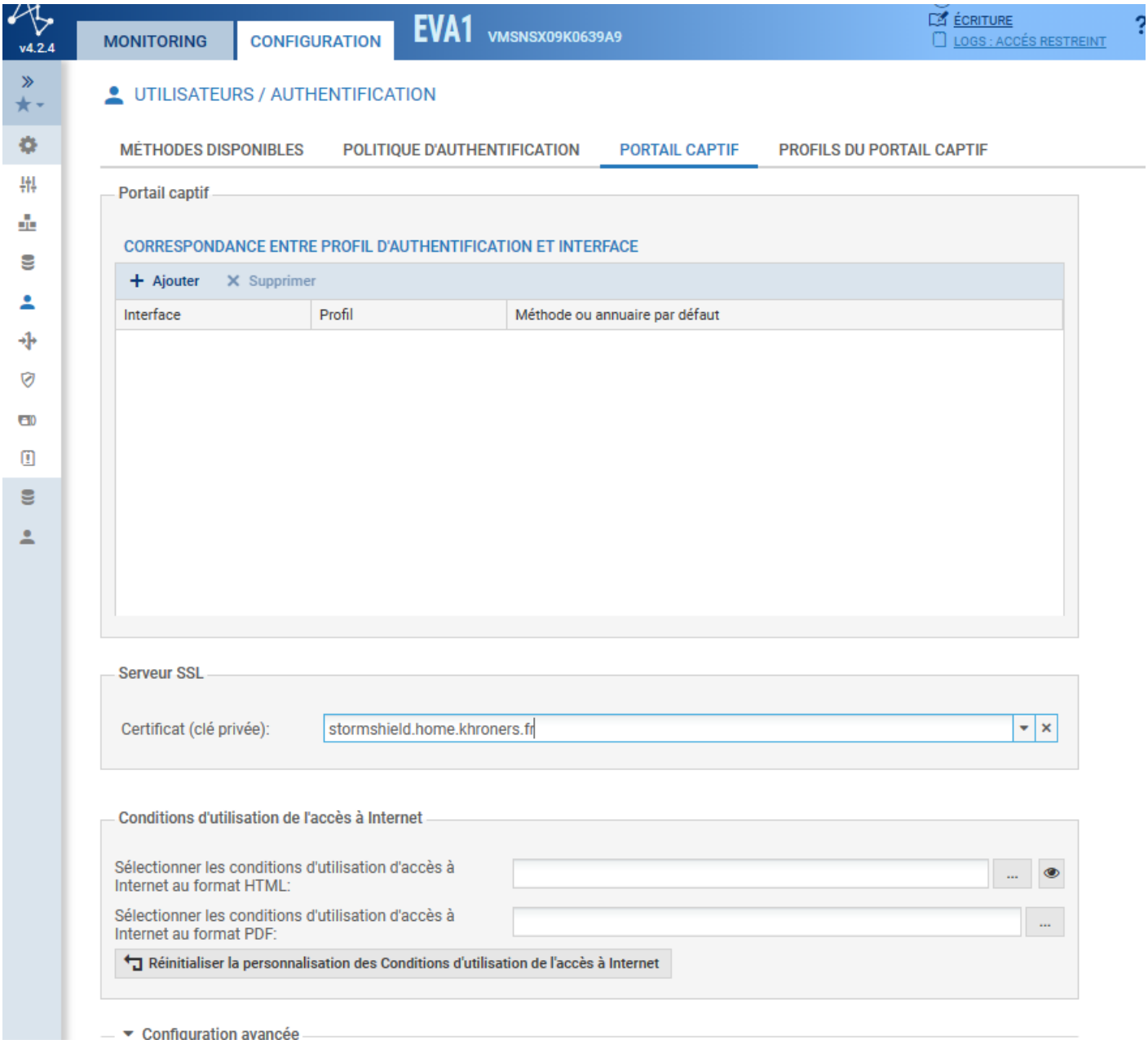
Ensuite, en CLI ou via l'interface web (on privilégie le CLI), on soumet la demande :

```
certreq.exe -submit -attrib "CertificateTemplate:SNS" C:\CertRequests\SNS.csr
```

On importe le certificat en PEM :



Une fois importé, on le définit dans la config.


v4.2.4
MONITORING
CONFIGURATION
EVA1
VMSNSX09K0639A9
ÉCRITURE
LOGS : ACCÉS RESTREINT
UTILISATEURS / AUTHENTIFICATION
MÉTHODES DISPONIBLES
POLITIQUE D'AUTHENTIFICATION
PORTAIL CAPTIF
PROFILS DU PORTAIL CAPTIF
Portail captif
CORRESPONDANCE ENTRE PROFIL D'AUTHENTIFICATION ET INTERFACE
Ajouter
Supprimer
Interface
Profil
Méthode ou annuaire par défaut
Serveur SSL
Certificat (clé privée):
stormshield.home.khroners.fr
Conditions d'utilisation de l'accès à Internet
Sélectionner les conditions d'utilisation d'accès à Internet au format HTML:
Sélectionner les conditions d'utilisation d'accès à Internet au format PDF:
Réinitialiser la personnalisation des Conditions d'utilisation de l'accès à Internet
Configuration avancée