

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

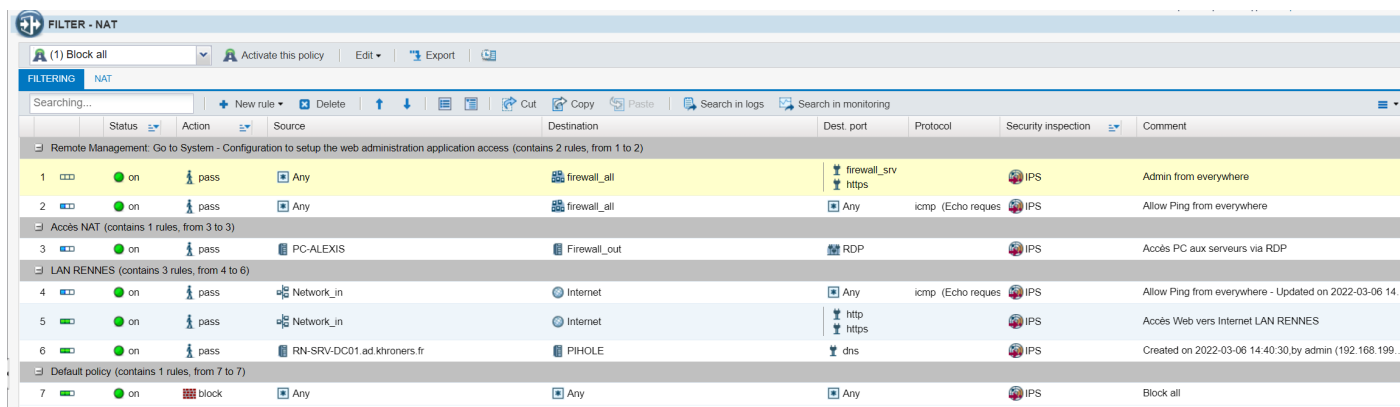
Filtrage de base

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.



	Status	Action	Source	Destination	Dest. port	Protocol	Security inspection	Comment
Remote Management: Go to System - Configuration to setup the web administration application access (contains 2 rules, from 1 to 2)								
1	on	pass	Any	firewall_all	firewall_srv https		IPS	Admin from everywhere
2	on	pass	Any	firewall_all		icmp (Echo request)	IPS	Allow Ping from everywhere
Accès NAT (contains 1 rules, from 3 to 3)								
3	on	pass	PC-ALEXIS	Firewall_out		RDP	IPS	Accès PC aux serveurs via RDP
LAN RENNES (contains 3 rules, from 4 to 6)								
4	on	pass	Network_in	Internet		icmp (Echo request)	IPS	Allow Ping from everywhere - Updated on 2022-03-06 14...
5	on	pass	Network_in	Internet		http https	IPS	Accès Web vers Internet LAN RENNES
6	on	pass	RN-SRV-DC01.ad.khroners.fr	PIHOLE		dns	IPS	Created on 2022-03-06 14:40:30 by admin (192.168.199...
Default policy (contains 1 rules, from 7 to 7)								
7	on	block	Any	Any			IPS	Block all

Pour avoir un fonctionnement "normal" dès le départ, on crée 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.

(1) Block all

Activate this policy

FILTERING

NAT

Searching...

New rule

Delete

↑

↓

Cut

Copy

Paste

Search in logs

Search in monitoring

		Status	Original traffic (before translation)				Traffic after translation				Protocol
			Source	Destination	Dest. port		Source	Src. port	Destination	Dest. port	
1		on	Any interface: out	Firewall_out	RDP3390	→	Firewall_in	RDP3390	RN-SRV-D	RDP3390	
2		on	Any interface: out	Firewall_out	RDP3391	→	Firewall_in	RDP3391	RN-SRV-D	RDP3391	
3		on	Any interface: out	Firewall_out	RDP3392	→	Firewall_in	RDP3392	RN-SRV-W	RDP3392	
4		off	Any interface: out	Firewall_out	RDP3393	→	Firewall_in	RDP3393	RN-SRV-W	RDP3393	
5		on	Any interface: out	Firewall_out	RDP3394	→	Firewall_in	RDP3394	RN-SRV-W	RDP3394	
6		on	Network_	Internet interface: out	Any	→	Firewall_out	ephemeral_fv	Internet		

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 :

	Status	Original traffic (before translation)			Traffic after translation			
		Source	Destination	Dest. port	Source	Src. port	Destination	Dest. port
1	on	Any interface: out	Firewall_out	RDP3390	Firewall_in	RDP3390	RN-SRV-D	RDP3390

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**" :

2	on	pass	PC-ALEXIS interface: out	Firewall_out	RDP	IPS
---	----	------	--------------------------	--------------	-----	-----

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.

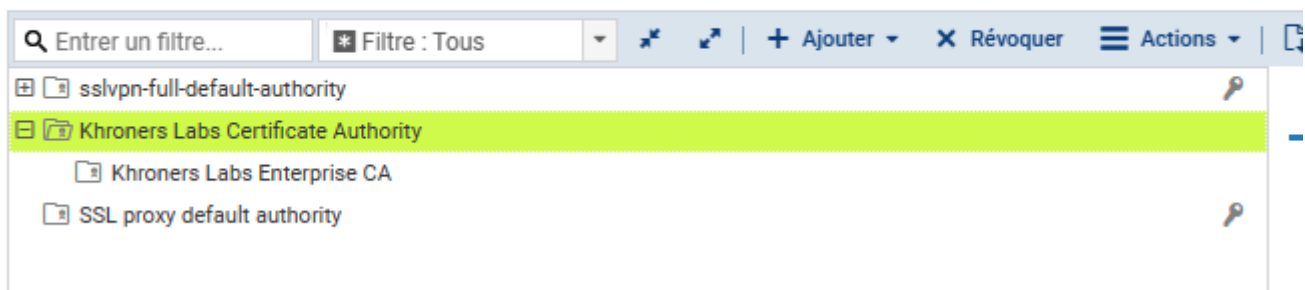
Dans mon cas :

FILTERING NAT										
Searching...		New rule Delete Up Down List Copy Paste Search in logs Search in monitoring								
	Status	Original traffic (before translation)			Traffic after translation				Protocol	Options
		Source	Destination	Dest. port	Source	Src. port	Destination	Dest. port		
1	on	Any interface: out	Firewall_out	RDP3390	Firewall_in	RDP3390	RN-SRV-DC01.ε	RDP3390		
2	on	Any interface: out	Firewall_out	RDP3391	Firewall_in	RDP3391	RN-SRV-DC02.ε	RDP3391		
3	on	Any interface: out	Firewall_out	RDP3392	Firewall_in	RDP3392	RN-SRV-WDS0.	RDP3392		
4	on	Any interface: out	Firewall_out	RDP3394	Firewall_in	RDP3394	RN-SRV-WS-AA	RDP3394		
5	on	Network_int	Internet interface: out	Any	Firewall_in	ephemeral_fw	Any			

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.

OBJETS / CERTIFICATS ET PKI



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 :

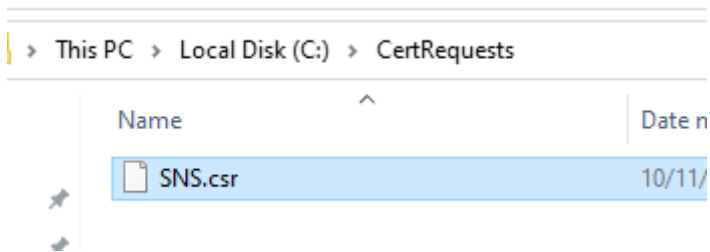
```
PKI REQUEST GET name=sns.home.khroners.fr-20231110 format=pem
```

TÉLÉCHARGEMENT DE FICHIER

Le fichier est disponible via le lien ci-dessous.
(Remarque : ces téléchargements ne supportent pas les extensions de téléchargement installées sur le navigateur)

[Télécharger VMSNSX09K0639A9](#)

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



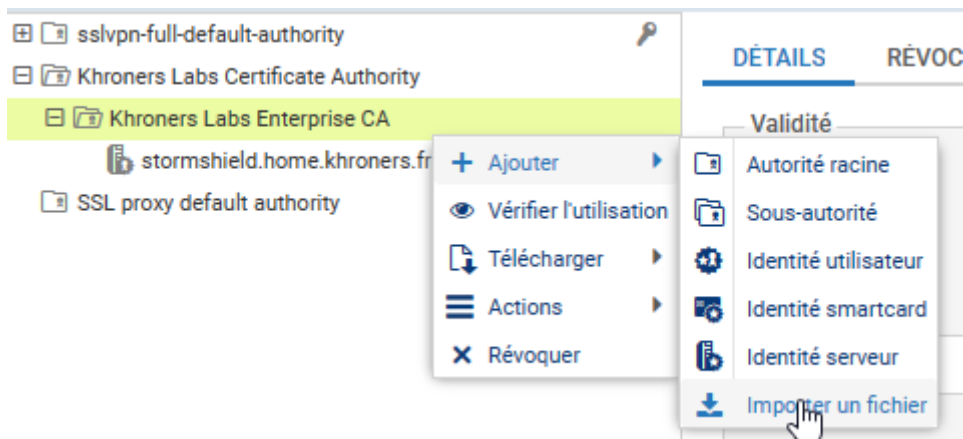
Dans AD CS, on crée notre modèle comme ici : [Creating a Microsoft Certificate Authority Template for SSL certificate creation in vSphere 6.x/7.x \(2112009\)](#).

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 : ACCÈS 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):

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