

# Règles de base

Règles de base Stormshield

- [Filtrage de base](#)
- [NAT](#)

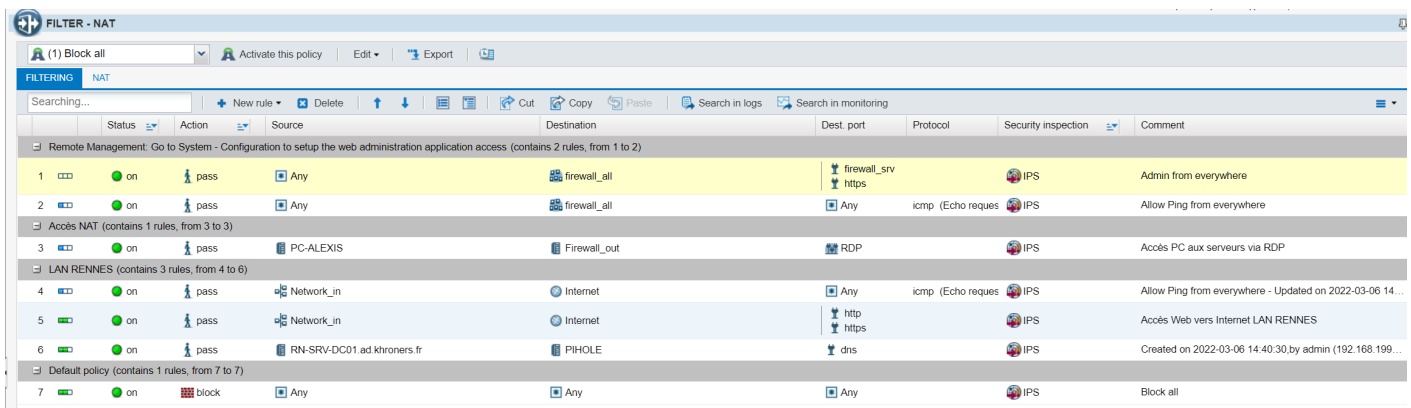
# Filtrage de base

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 14:40:30 by admin (192.168.199.1)
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 (192.168.199.1)
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	<div><div></div><div>on</div></div>	<div><div></div>Any interface: out</div>	<div><div></div>Firewall_out</div>	<div><div></div>RDP3390</div>	→	<div><div></div>Firewall_in</div>	<div><div></div>RDP3390</div>	<div><div></div>RN-SRV-D</div>	<div><div></div>RDP3390</div>	
2	<div><div></div><div>on</div></div>	<div><div></div>Any interface: out</div>	<div><div></div>Firewall_out</div>	<div><div></div>RDP3391</div>	→	<div><div></div>Firewall_in</div>	<div><div></div>RDP3391</div>	<div><div></div>RN-SRV-D</div>	<div><div></div>RDP3391</div>	
3	<div><div></div><div>on</div></div>	<div><div></div>Any interface: out</div>	<div><div></div>Firewall_out</div>	<div><div></div>RDP3392</div>	→	<div><div></div>Firewall_in</div>	<div><div></div>RDP3392</div>	<div><div></div>RN-SRV-W</div>	<div><div></div>RDP3392</div>	
4	<div><div></div><div>off</div></div>	<div><div></div>Any interface: out</div>	<div><div></div>Firewall_out</div>	<div><div></div>RDP3393</div>	→	<div><div></div>Firewall_in</div>	<div><div></div>RDP3393</div>	<div><div></div>RN-SRV-W</div>	<div><div></div>RDP3393</div>	
5	<div><div></div><div>on</div></div>	<div><div></div>Any interface: out</div>	<div><div></div>Firewall_out</div>	<div><div></div>RDP3394</div>	→	<div><div></div>Firewall_in</div>	<div><div></div>RDP3394</div>	<div><div></div>RN-SRV-W</div>	<div><div></div>RDP3394</div>	
6	<div><div></div><div>on</div></div>	<div><div></div>Network_</div>	<div><div></div>Internet interface: out</div>	<div><div></div>Any</div>	→	<div><div></div>Firewall_out</div>	<div><div></div>ephemeral_fw</div>	<div><div></div>Internet</div>		

Tout le trafic du LAN vers Internet sera translaté.