

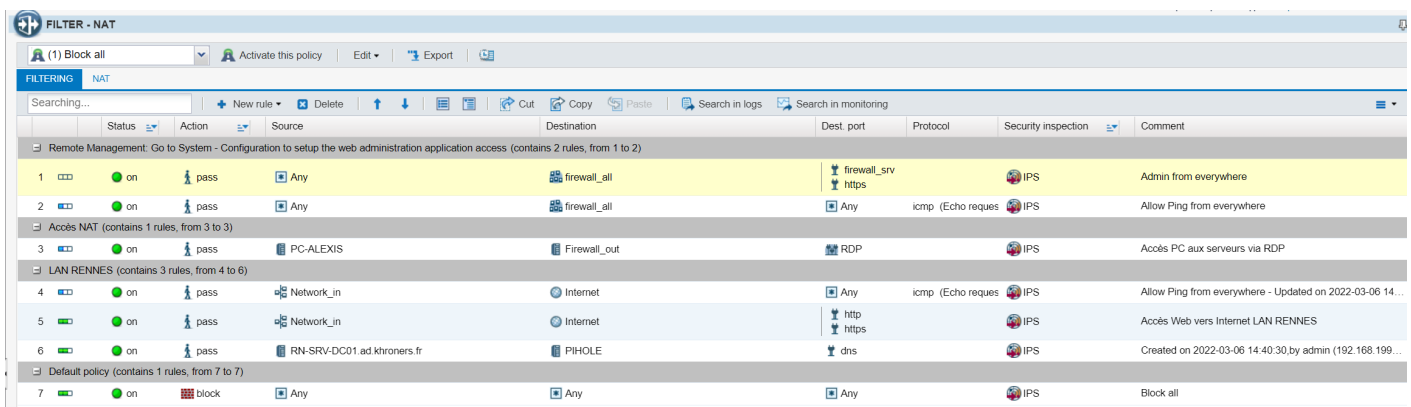
Filtrage de base

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	Any	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	Any	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	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.

Revision #2

Created 3 March 2022 19:34:06 by Khroners

Updated 6 March 2022 14:28:13 by Khroners