Règles de base

Règles de base Stormshield

- Filtrage de base
- NAT

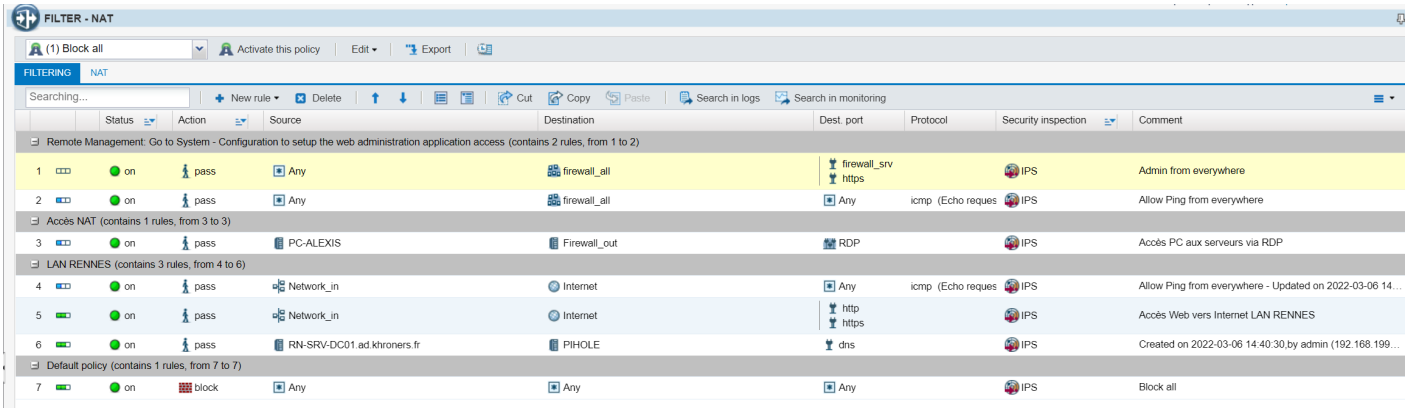
Filtrage de base

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.



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.

(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_fw	Internet		

Tout le trafic du LAN vers Internet sera translaté.