Pare Feu – Stormshield

1. Contexte et Plan d'Adressage

Contexte :

Agence	ID VLAN	Adresses de sous-réseaux	Adresses IP de votre firewall Stormshield
Johannesburg	333	**DMZ :** 172.16.10.0/24	**dmz :** 172.16.10.254
	334	**SERVEURS :** 172.16.30.0/24	**dmz :** 172.16.30.254
	335	**LAN :** 192.168.10.0/24	**in/lan :** 192.168.10.254
	302	**WAN :** 192.168.229.0/24	**out :** 192.168.229.33

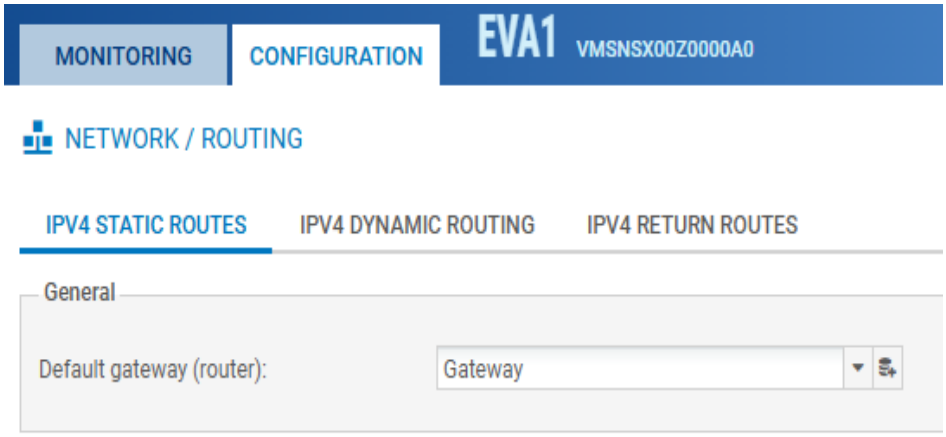
2. Mise en Place du Réseau

La configuration des interfaces s'effectue dans le menu Configuration / Réseau / Interfaces

Les Interfaces :

Route par défaut :

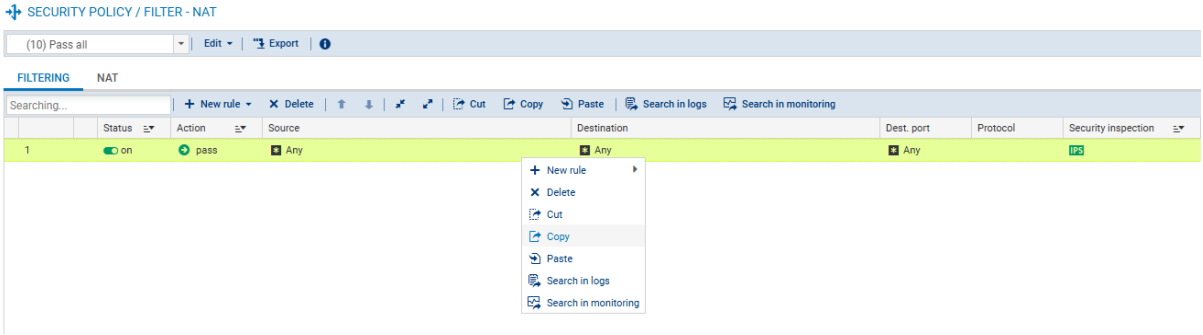
Le pare-feu SNS local doit utiliser l'adresse IP du pare-feu SNS du siège, soit `192.168.229.1`, comme passerelle par défaut.



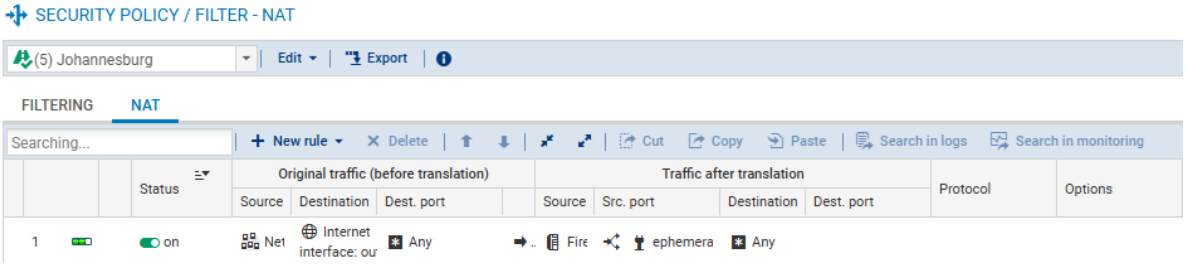
3. Mise en Œuvre de la Translation d'Adresses (NAT/PAT)

Il faut ouvrir le menu **Configuration / Politique de sécurité / Filtrage et NAT**

Puis Il faut copier le filtrage de la rubrique 10 Pass all



Puis ensuite coller le filtre dans la rubrique 5 Johannesburg (dans son agence)



Maintenant, il faut éditez cette règle en double cliquant dessus :

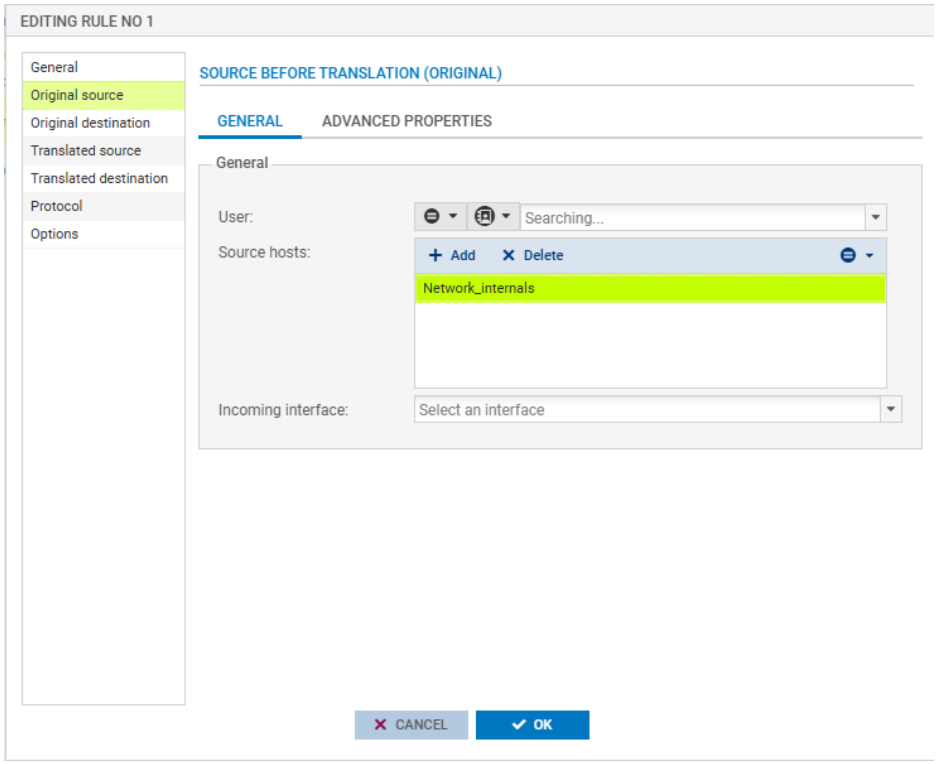
Editez la règle :

Double-cliquer sur une zone vide de la règle pour ouvrir la fenêtre de configuration détaillée *« Édition de la règle N°1 »*.

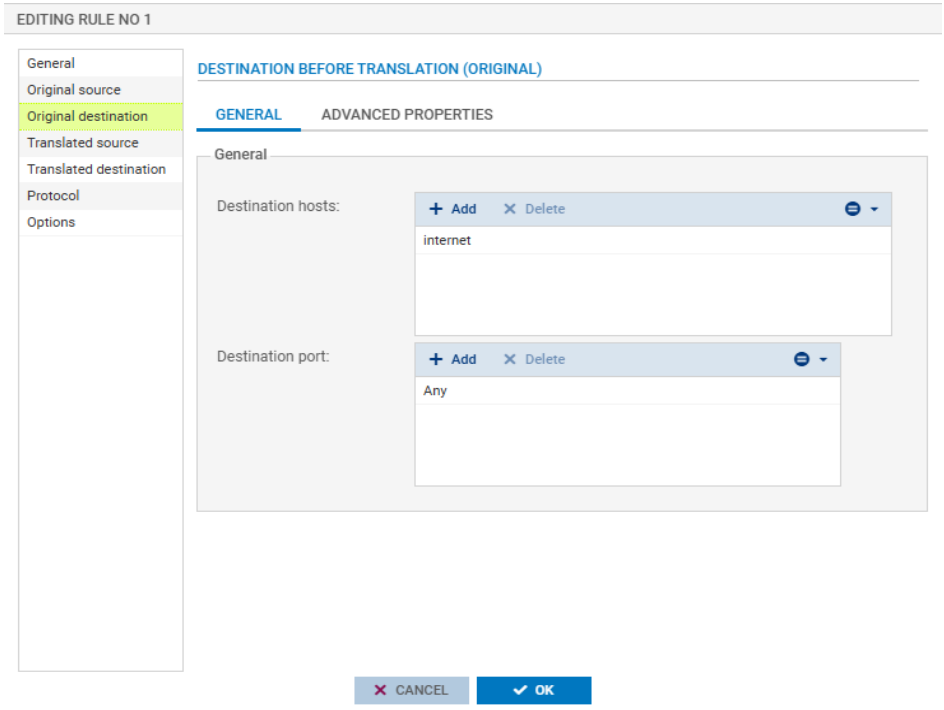
Définir la source originale :

Cliquer sur l'onglet **Source originale** (menu de gauche).

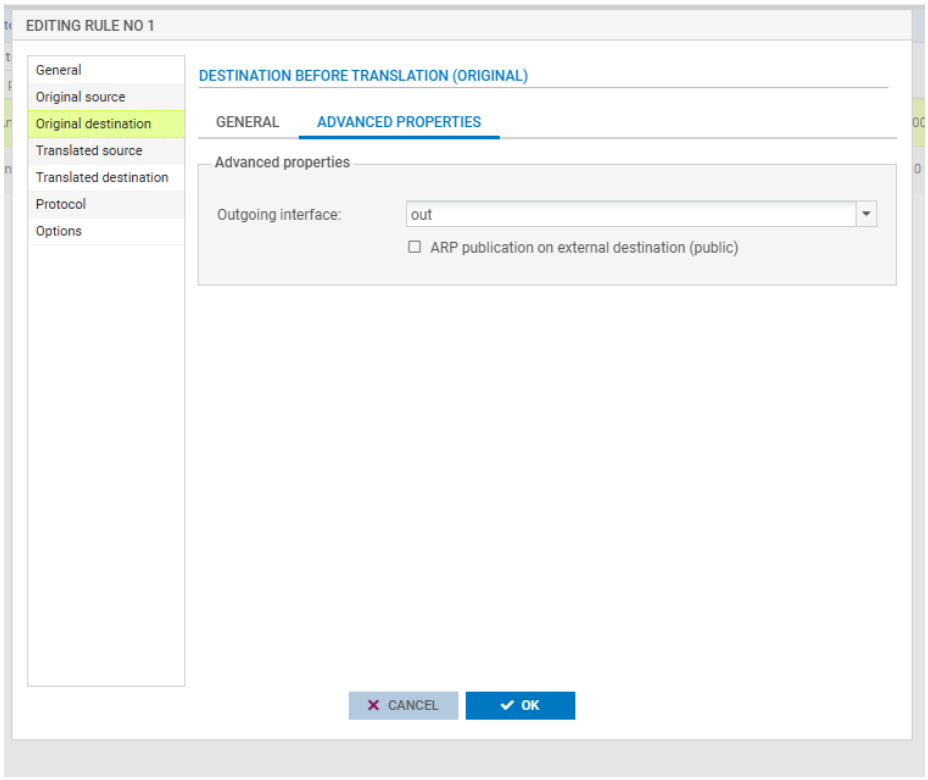
Double-cliquer sur **Any** puis, avec la flèche, choisir **Network_internals** (qui renvoie à tous les réseaux internes protégés).



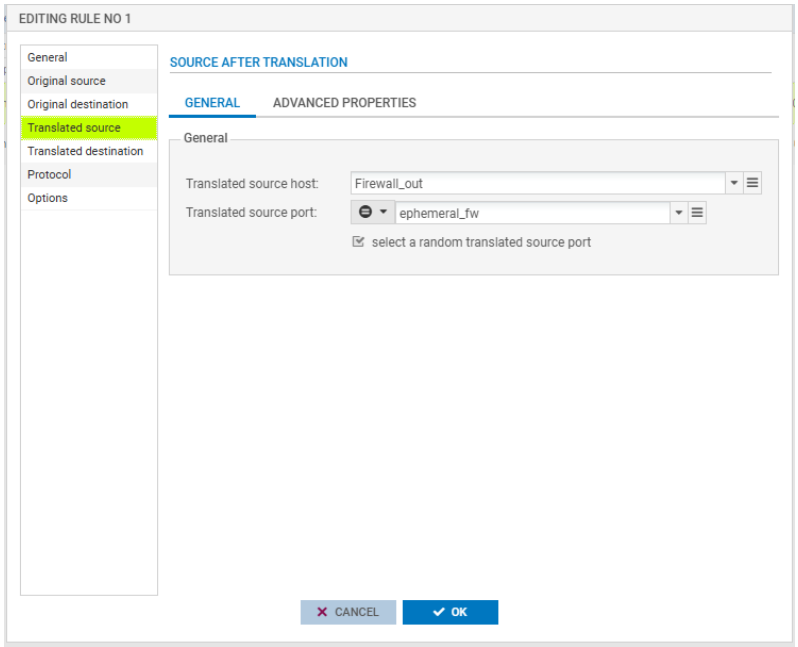
Dans l'onglet **Configuration avancée**, laisser **Any** pour le port de destination et mettre Internet dans la destination host



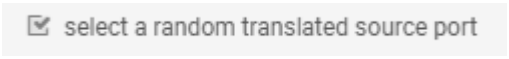
Puis dans le même onglet cliquer sur Advanced Properties , et mettre OUT en interface de sortie



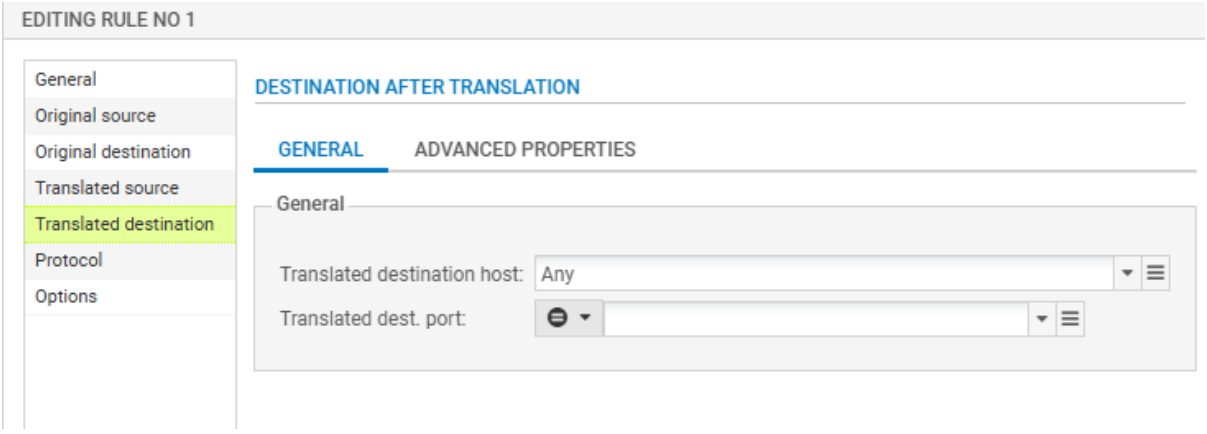
Ensuite cliquer sur l'onglet Translated source puis sélectionner Firewall_Out dans translated source host.



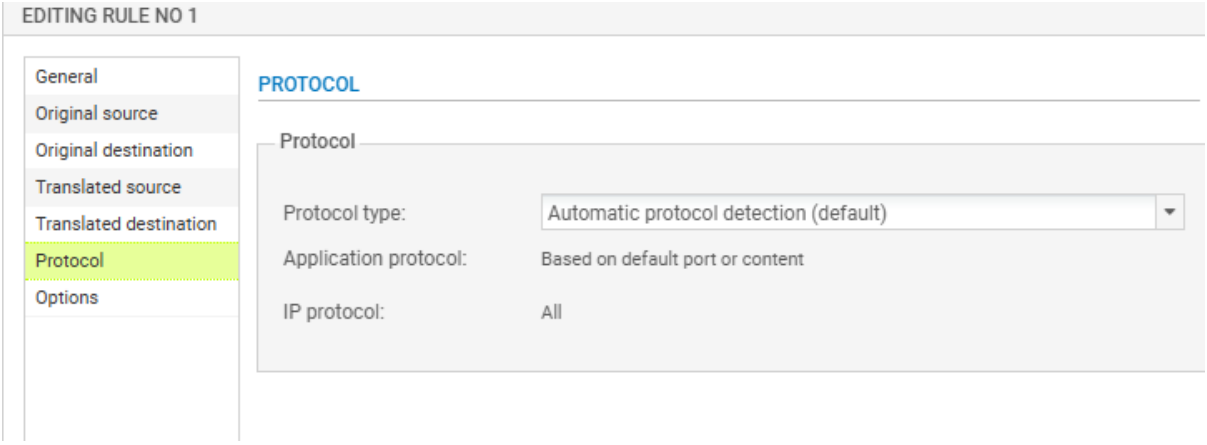
Puis dans Translated source port, laisser ephemeral_fw et cocher choisir aléatoirement le port source translaté.



Ensuite dans translated destination laissez Any

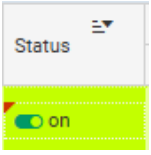


Maintenant il faut aller dans l'onglet Protocol et laissez par défaut détection automatique



Puis sauvegarder les changements et quittez

Et activé la règle en cliquer sur ON



SECURITY POLICY / FILTER - NAT

(5) Johannesburg | Edit | Export

FILTERING NAT

Searching... | New rule | Delete | Cut | Copy | Paste | Search in logs | Search in monitoring

		Status	Action	Source	Destination	Dest. port	Protocol	Security inspection	Comments
1		off	pass	Any	Any	Any		IPS	Créé le 2025-10-07 08:45:44 par admin (10.187.35.153)
Section 1 Règles d'autorisation à destination du pare-feu (contains 2 rules, from 2 to 3)									
2		on	pass	Internet	firewall_all	firewall_srv https		IPS	Admin from everywhere - Mis à jour le 2025-09-22 13:35:46 par a...
3		on	block	Internet	Firewall_out	dns		IPS	Créé le 2025-09-25 14:32:50 par admin (10.187.35.141)
Separator - Règles d'autorisation des flux métiers (contains 11 rules, from 4 to 14)									
4		on	pass	inter @ Internet	Firewall_out	rdp		IPS	Créé le 2025-11-06 14:34:26 par admin (10.187.35.132)
5		on	pass	Network_internals	Internet	https http		IPS	Créé le 2025-09-22 13:22:20 par admin (10.187.35.185)
6		on	pass	Network_internals	Internet	Any	icmp	IPS	Créé le 2025-09-22 13:22:20 par admin (10.187.35.185) - Mis à jo...
7		off	pass	Network_internals	Internet	dns		IPS	Créé le 2025-09-22 13:22:20 par admin (10.187.35.185) - Mis à jo...
8		on	pass	Network_internals	DC-01	ldap		IPS	Créé le 2025-11-13 16:08:17 par admin (10.187.35.134)
9		on	pass	Network_internals	DC-01	kerberos		IPS	Créé le 2025-11-13 16:08:17 par admin (10.187.35.134) - Mis à jo...
10		on	pass	AgentRelais	ServeurDHCP	bootps		IPS	Created on 2025-09-23 07:13:46 by admin (10.187.35.159)
11		on	pass	dns0	Internet	dns		IPS	Créé le 2025-11-13 15:35:06 par admin (10.187.35.134)
12		on	pass	Network_internals	Firewall_all	Any	icmp	IPS	Créé le 2025-11-13 16:23:40 par admin (10.187.35.134)
13		on	pass	Network_dmz2 Network_dmz1	dns0	dns		IPS	Créé le 2025-11-13 16:32:25 par admin (10.187.35.134)
14		on	pass	dns0	ns0	dns		IPS	Créé le 2025-11-13 15:37:00 par admin (10.187.35.134)
Section 6 Block All (contains 1 rules, from 15 to 15)									
15		on	block	Any	Any	Any		IPS	Block all - Mis à jour le 2025-09-22 13:36:56 par admin (10.187.3...