

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

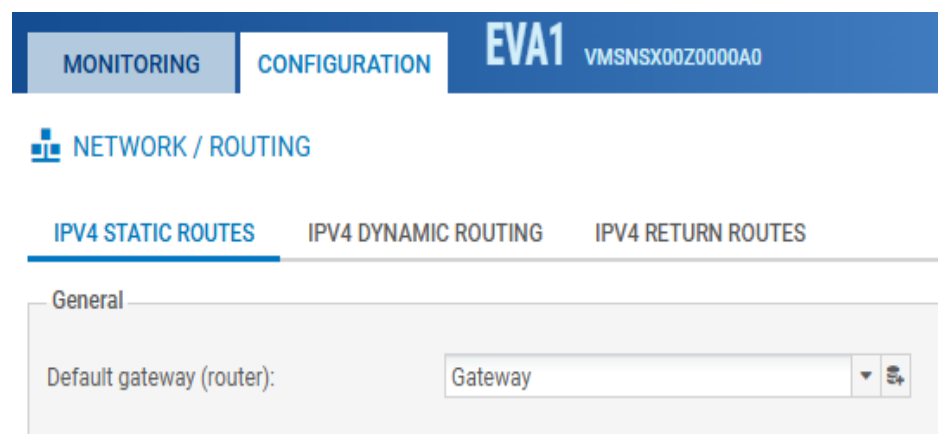
Les Interfaces :

 out	IPv4 address
 in	192.168.229.33/24
 dmz1	192.168.10.254/24
 dmz2	172.16.10.254/24
 Admin	172.16.30.254/24
	10.187.35.196/24 (DHCP)

---->

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.

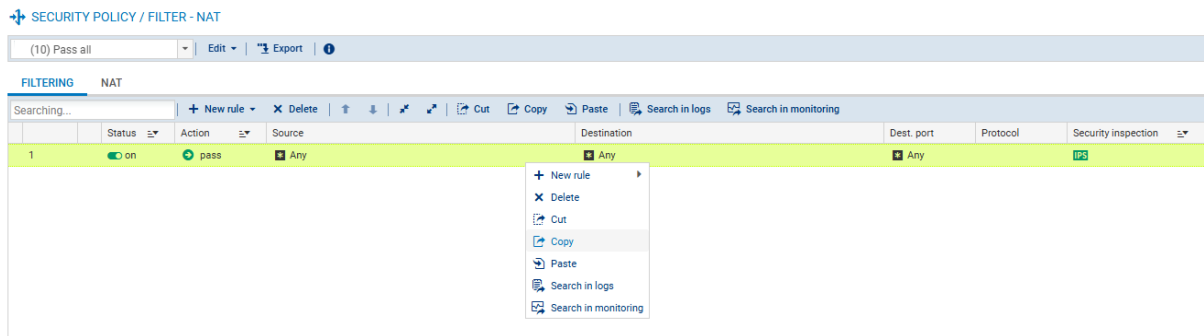


The screenshot shows the Fortinet configuration interface. At the top, there are tabs for 'MONITORING' and 'CONFIGURATION', with 'CONFIGURATION' selected. To the right, the device name 'EVA1' and its serial number 'VMSNSX00Z0000A0' are displayed. Below the tabs, the 'NETWORK / ROUTING' section is active. Under this section, there are three sub-tabs: 'IPV4 STATIC ROUTES', 'IPV4 DYNAMIC ROUTING', and 'IPV4 RETURN ROUTES'. The 'IPV4 STATIC ROUTES' tab is selected. Within this tab, the 'General' section is visible. It contains a label 'Default gateway (router):' followed by a text input field containing the word 'Gateway'. To the right of the input field is a dropdown arrow and a small icon representing a network diagram.

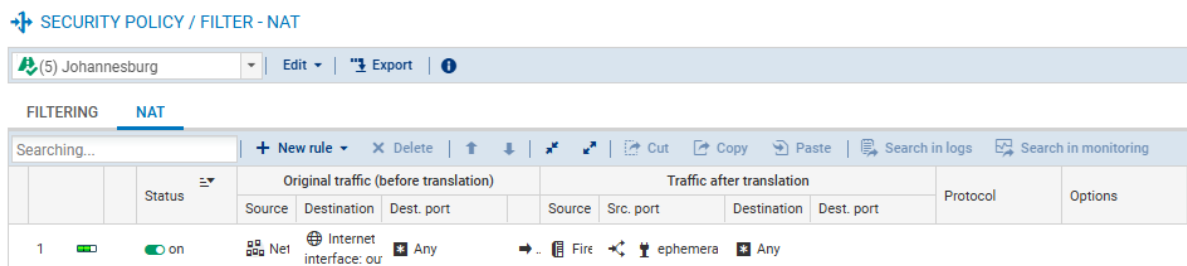
3. Mise en Œuvre de la Translation d'Adresses (NAT/PAT)

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).

EDITING RULE NO 1

General

Original source

Original destination

Translated source

Translated destination

Protocol

Options

SOURCE BEFORE TRANSLATION (ORIGINAL)

GENERAL

ADVANCED PROPERTIES

General

User:

Searching...

Source hosts:

+ Add

✕ Delete

Network_Internals

Incoming interface:

Select an interface

✕ CANCEL

✓ OK

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

EDITING RULE NO 1

General

Original source

Original destination

Translated source

Translated destination

Protocol

Options

DESTINATION BEFORE TRANSLATION (ORIGINAL)

GENERAL

ADVANCED PROPERTIES

General

Destination hosts:

+ Add

✕ Delete

internet

Destination port:

+ Add

✕ Delete

Any

✕ CANCEL

✓ OK

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

The screenshot shows the 'EDITING RULE NO 1' window with the 'ADVANCED PROPERTIES' tab selected. The left sidebar lists 'General', 'Original source', 'Original destination', 'Translated source', 'Translated destination', 'Protocol', and 'Options'. The main area is titled 'DESTINATION BEFORE TRANSLATION (ORIGINAL)' and contains an 'Advanced properties' section. In this section, the 'Outgoing interface' is set to 'out' in a dropdown menu, and the checkbox for 'ARP publication on external destination (public)' is unchecked. At the bottom are 'CANCEL' and 'OK' buttons.

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

The screenshot shows the 'EDITING RULE NO 1' window with the 'Translated source' tab selected. The left sidebar lists 'General', 'Original source', 'Original destination', 'Translated source', 'Translated destination', 'Protocol', and 'Options'. The main area is titled 'SOURCE AFTER TRANSLATION' and contains a 'General' section. In this section, the 'Translated source host' is set to 'Firewall_out' in a dropdown menu, and the 'Translated source port' is set to 'ephemeral_fw' in a dropdown menu. The checkbox for 'select a random translated source port' is checked. At the bottom are 'CANCEL' and 'OK' buttons.

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

☒ select a random translated source port

Ensuite dans translated destination laissez Any

EDITING RULE NO 1

General	DESTINATION AFTER TRANSLATION
Original source	
Original destination	
Translated source	
Translated destination	
Protocol	
Options	

GENERAL ADVANCED PROPERTIES

General

Translated destination host: Any

Translated dest. port:

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

EDITING RULE NO 1

General	PROTOCOL
Original source	
Original destination	
Translated source	
Translated destination	
Protocol	
Options	

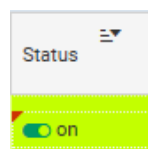
Protocol

Protocol type: Automatic protocol detection (default)

Application protocol: Based on default port or content

IP protocol: All

Puis sauvegarder les changements et quittez



Et activé la règle en cliquant sur ON

(5) Johannesburg

Edit | Export |

FILTERING NAT

Searching...

+ New rule | X Delete | ↑ ↓ ↶ ↷ ⌂ Cut Copy Paste | 🔍 Search in logs 🔍 Search in monitoring

	Status	Action	Source	Destination	Dest. port	Protocol	Security inspection	Comments
1		pass	Any	Any	Any			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		pass	Internet	firewall_all	firewall_srv https			Admin from everywhere - Mis à jour le 2025-09-22 13:35:46 par a...
3		block	Internet	Firewall_out	dns			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		pass	inter @ Internet	Firewall_out	rdp			Créé le 2025-11-06 14:34:26 par admin (10.187.35.132)
5		pass	Network_internals	Internet	https http			Créé le 2025-09-22 13:22:20 par admin (10.187.35.185)
6		pass	Network_internals	Internet	Any	icmp		Créé le 2025-09-22 13:22:20 par admin (10.187.35.185) - Mis à jo...
7		pass	Network_internals	Internet	dns			Créé le 2025-09-22 13:22:20 par admin (10.187.35.185) - Mis à jo...
8		pass	Network_internals	DC-01	ldap			Créé le 2025-11-13 16:08:17 par admin (10.187.35.134)
9		pass	Network_internals	DC-01	kerberos			Créé le 2025-11-13 16:08:17 par admin (10.187.35.134) - Mis à jo...
10		pass	AgentRelais	ServeurDHCP	bootps			Created on 2025-09-23 07:13:46 by admin (10.187.35.159)
11		pass	dns0	Internet	dns			Créé le 2025-11-13 15:35:06 par admin (10.187.35.134)
12		pass	Network_internals	Firewall_all	Any	icmp		Créé le 2025-11-13 16:23:40 par admin (10.187.35.134)
13		pass	Network_dmz2 Network_dmz1	dns0	dns			Créé le 2025-11-13 16:32:25 par admin (10.187.35.134)
14		pass	dns0	ns0	dns			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		block	Any	Any	Any			Block all - Mis à jour le 2025-09-22 13:36:56 par admin (10.187.3...