NOTE TECHNIQUE

STORMSHIELD NETWORK SECURITY

RÉPARTITION DE TRAFIC SUR PLUSIEURS FIREWALLS

Produits concernés : SNS 3.x, SNS 4.x

Dernière mise à jour du document : 09 décembre 2019

Référence : sns-fr-stacking_répartition_de_trafic_sur_plusieurs_firewalls_note_technique

Table des matières

Avant de commencer 4

Architectures présentées 5

Cas 1 : répartition de tunnels VPN IPsec 5
Cas 2 : répartition de proxies 6

Cas 1 : répartition de tunnels IPsec 7

Paramétrer le firewall FWA1 7
Créer une interface virtuelle IPsec 7
Définir une route vers le réseau distant 7
Définir les routes de retour 7
Définir la répartition de charge 8
Mettre en œuvre la règle de filtrage 9
Mettre en œuvre la politique IPsec 10
Paramétrer le firewall FWA2 10
Créer une interface virtuelle IPsec 11
Définir une route vers le réseau distant 11
Définir les routes de retour 11
Mettre en œuvre la règle de filtrage 12
Mettre en œuvre la politique IPsec 12
Paramétrer le firewall FWA3 13
Créer une interface virtuelle IPsec 13
Définir une route vers le réseau distant 13
Définir les routes de retour 13
Mettre en œuvre la règle de filtrage 14
Mettre en œuvre la politique IPsec 14
Paramétrer le firewall FWB1 15
Créer une interface virtuelle IPsec 15
Définir une route vers le réseau distant 15
Définir les routes de retour 15
Mettre en œuvre la règle de filtrage 16
Mettre en œuvre la politique IPsec 16
Paramétrer le firewall FWB2 16
Créer une interface virtuelle IPsec 16
Définir une route vers le réseau distant 17
Définir les routes de retour 17
Mettre en œuvre la règle de filtrage 17
Mettre en œuvre la politique IPsec 17
Paramétrer le firewall FWB3 18
Créer une interface virtuelle IPsec 18
Définir une route vers le réseau distant 18
Définir les routes de retour 18
Mettre en œuvre la règle de filtrage 18
Mettre en œuvre la politique IPsec 19

Cas 2 : répartition de proxies 20

Paramétrer le Firewall FW1 20
Définir une route vers le réseau distant 20
Définir les routes de retour 20
Définir la répartition de charge 21
Mettre en œuvre la règle de filtrage 22

Paramétrer le Firewall FW2 23
Définir une route vers le réseau distant 23
Définir une route de retour 24
Activer le proxy SSL dans la règle de filtrage 24
Paramétrer les Firewalls FW3 et FW4 25
Définir une route vers le réseau distant 25
Définir une route de retour 25
Activer le proxy HTTP dans la règle de filtrage 25
Paramétrer le Firewall FW5 26
Définir une route vers le réseau distant 26
Définir une route de retour 26
Activer le proxy SMTP dans la règle de filtrage 27
Paramétrer le Firewall FW6 27
Routes de retour 27
Mettre en œuvre une règle de filtrage 28
Mettre en œuvre une règle de translation d'adresses (NAT) 28

Pour aller plus loin 30

Avant de commencer

Depuis la version 2 de firmware, les firewalls Stormshield Network ont été enrichis de deux nouvelles fonctionnalités liées au mécanisme de routage: les objets routeurs et les routes de retour.

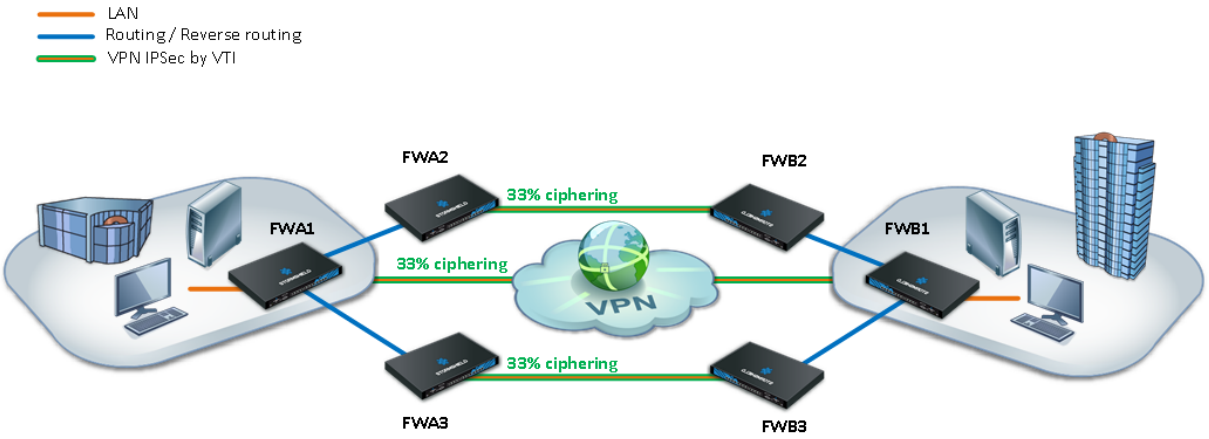
Ces fonctionnalités permettent ainsi une configuration plus simple et plus intuitive du routage et de la répartition de charge, facilitant ainsi la mise en place d'architectures sophistiquées.

Cette note technique présente deux exemples d'implémentation de ces fonctionnalités, afin de répartir le trafic sur plusieurs firewalls, optimisant ainsi les performances et l'utilisation de la bande passante.

Architectures présentées

Deux exemples de répartition de flux sont présentés dans ce document :

Cas 1 : répartition de tunnels VPN IPsec

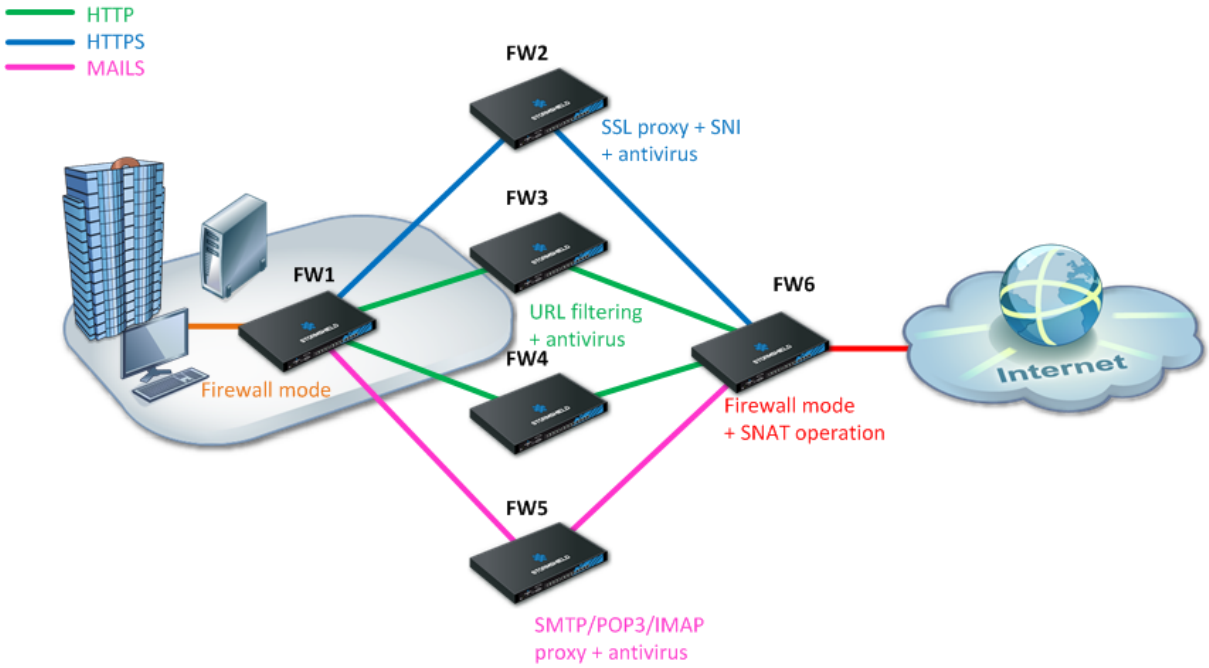


Le premier cas proposé dans cette note technique utilise les objets routeurs et routes de retour afin de distribuer les tunnels IPsec sur plusieurs firewalls, répartissant ainsi les ressources système nécessaires au chiffrement / déchiffrement des données.

Les tunnels IPsec sont ici basés sur des interfaces virtuelles IPsec (VTI - cf. note technique *Interfaces virtuelles IPsec*) afin de permettre une décision de chiffrement basée sur le routage, et non plus sur la Security Policy Database (SPD), grâce à la notion d'objets routeurs. Les routes de retour assurent quant à elles le routage des paquets réponse vers le firewall émetteur.

Les exemples de configuration présentés dans cette note technique supposent des flux initiés depuis le site A et à destination du site B.

Cas 2 : répartition de proxies



Le deuxième cas présenté dans ce document utilise les objets routeurs et les routes de retour afin de répartir les flux en fonction de leur nature (SSL, HTTP et messagerie) vers des proxies activés sur des firewalls distincts.

Dans la politique de filtrage, le routage des flux selon le protocole repose ici aussi sur l'utilisation d'objets routeurs. Les routes de retour assurent quant à elles le routage des paquets réponse vers le firewall émetteur.

Cas 1 : répartition de tunnels IPsec

Paramétrer le firewall FWA1

Le paramétrage de FWA1 consiste à :

- Créer une interface virtuelle IPsec,
- Définir une route vers le réseau distant,
- Définir les routes de retour,
- Définir la répartition de charge,
- Mettre en œuvre la règle de filtrage,
- Mettre en œuvre la politique IPsec.

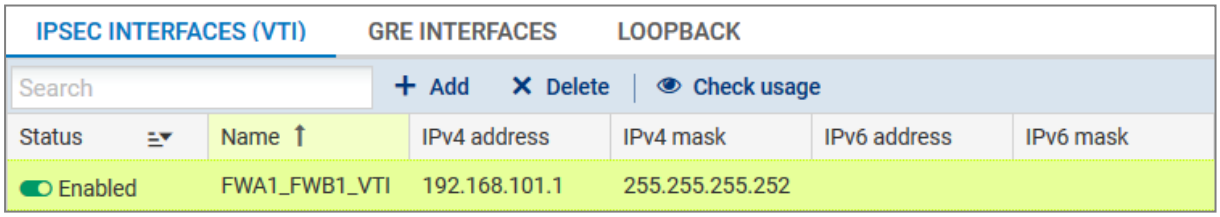
Créer une interface virtuelle IPsec

Créez l'interface virtuelle sur laquelle sera basé le tunnel IPsec entre le firewall 1 du site A (FWA1) et le firewall 1 du site B (FWB1).

Dans le module **Configuration** > **Réseau**>**Interfaces virtuelles**, sur l'onglet *Interfaces IPsec (VTI)*, cliquez sur le bouton **Ajouter**.

Renseignez les champs obligatoires :

- **Nom** : FWA1_FWB1_VTI dans l'exemple,
- **Adresse IP** : 192.168.101.1 dans l'exemple,
- **Masque** : 255.255.255.252 dans l'exemple.



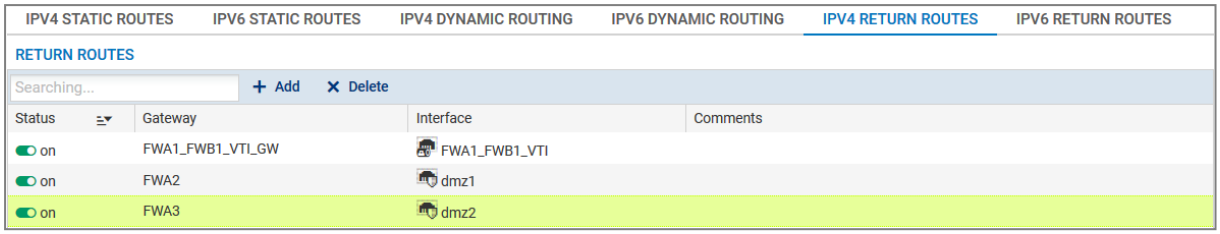
Définir une route vers le réseau distant

Bien que dans cette configuration le firewall effectue du routage au sein de la politique de filtrage (Policy Based Routing), il est **nécessaire de définir une route par défaut ou une route statique explicite vers le réseau distant**.

En effet, la première action effectuée par le firewall est de vérifier qu'il dispose d'une route vers le site distant avant de consulter sa politique de filtrage. L'absence de cette route provoquerait donc un rejet des paquets.

Définir les routes de retour

Créez 3 routes permettant d'acheminer les paquets retour vers le firewall d'origine grâce à l'adresse MAC source :



Route de retour vers le firewall FWB1

Dans le module **Configuration** > **Réseau** > **Routage**, sur l'onglet *Routes de retour*, cliquez sur le bouton **Ajouter**.

Renseignez les champs obligatoires :

- **Passerelle** : créez un objet réseau en cliquant sur l'icône . Celui-ci doit correspondre à l'interface virtuelle IPsec du firewall 1 du site B (FWA1_FWB1_VTI_GW ayant pour adresse IPv4 192.168.101.2 dans l'exemple),
- **Interface** : sélectionnez l'interface virtuelle locale définie pour le tunnel IPsec entre les firewalls 1 des sites A et B (FWA1_FWB1_VTI dans l'exemple).

Activez la route par un double clic dans la colonne **Etat**.

Route de retour vers le firewall FWA2

- **Passerelle** : créez l'objet réseau correspondant au firewall 2 du site A (FWA2 dans l'exemple),

> **NOTE**
> L'adresse MAC du firewall FWA2 doit impérativement être déclarée dans cet objet réseau.

- **Interface** : sélectionnez l'interface du firewall FWA1 par laquelle les paquets retour seront acheminés vers le firewall FWA2 (Dmz1 dans l'exemple).

Activez la route par un double clic dans la colonne **Etat**.

Route de retour vers le firewall FWA3

- **Passerelle** : créez l'objet réseau correspondant au firewall 3 du site A (FWA3 dans l'exemple),

> **NOTE**
> L'adresse MAC du firewall FWA3 doit impérativement être déclarée dans cet objet réseau.

- **Interface** : sélectionnez l'interface du firewall FWA1 par laquelle les paquets retour seront acheminés vers le firewall FWA3 (Dmz2 dans l'exemple).

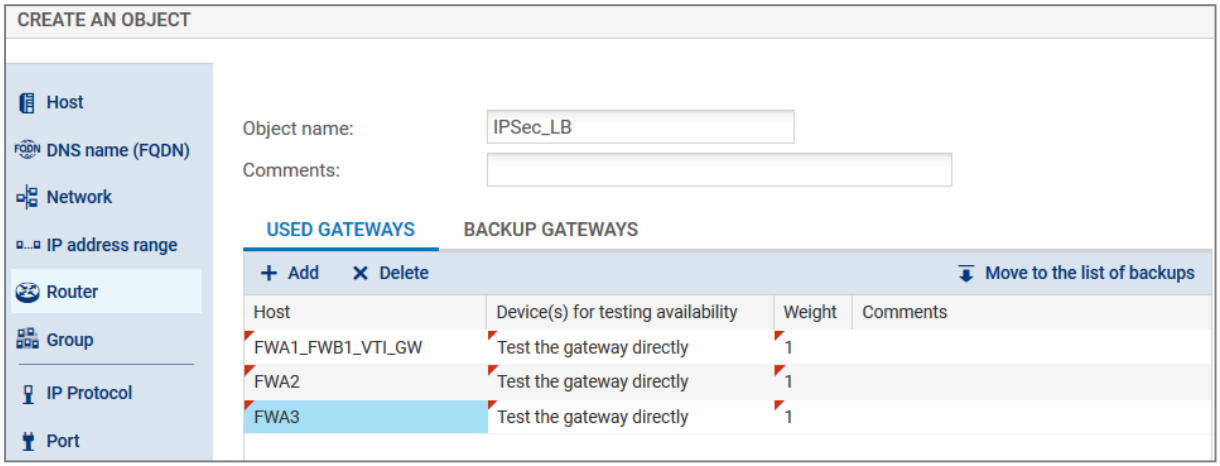
Activez la route par un double clic dans la colonne **Etat**.

Définir la répartition de charge

La répartition de charge des paquets destinés à être chiffrés dans les 3 tunnels IPsec est réalisée grâce à un objet routeur composé des firewalls FWA2, FWA3 et FWB1.

1. Dans le module **Configuration** > **Objets** > **Objets réseaux**, cliquez sur **Ajouter**.
2. Positionnez-vous sur le menu **Routeur**.

3. Indiquez un nom pour cet objet (IPsec_LB dans l'exemple).
4. Dans l'onglet *Passerelles utilisées*, cliquez sur **Ajouter** et sélectionnez l'objet réseau correspondant à l'interface virtuelle IPsec du firewall FWB1 (FWA1_FWB1_VTI_GW). Laissez la valeur **Tester directement la passerelle** pour la colonne *Test de la disponibilité*. De même, laissez la valeur **1** dans la colonne *Poids*.
5. Répétez cette opération pour ajouter les passerelles FWA2 et FWA3.



6. Dans le panneau Configuration avancée, vérifiez que les différents champs prennent les valeurs suivantes :
   - **Répartition de charge** : *Par connexion* (chaque nouvelle connexion devant être chiffrée dans un tunnel IPsec envoyée vers l'une des passerelles déclarées selon le principe du Round-Robin),
   - **Activation des passerelles de secours** : *Lorsque toutes les passerelles sont injoignables*,
   - **Activer toutes les passerelles de secours en cas d'indisponibilité** : décochée,
   - **Si aucune passerelle n'est disponible** : *Routage par défaut*.
7. Validez la création de l'objet routeur en cliquant sur le bouton **Créer**.

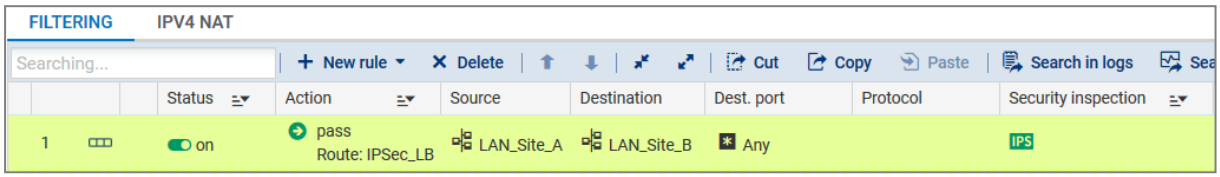
Mettre en œuvre la règle de filtrage

Pour que les flux soient répartis de manière égale entre les 3 firewalls (FWA1, FWA2 et FWA3) et transitent par leur tunnel IPsec respectif, créez une règle de filtrage. Celle-ci doit intégrer une directive de routage basée sur l'objet routeur créé précédemment.

1. Dans le menu **Configuration** > **Politique de sécurité** > **Filtrage et NAT**, double-cliquez dans la colonne **État** pour le passer à **On**.
2. Dans la colonne **Action**, double-cliquez pour choisir la valeur *passer* pour le champ **Action**. Sélectionnez dans le champ **Passerelle - routeur** l'objet routeur créé pour le partage de charge (IPsec_LB dans l'exemple).
3. Dans le menu **Source**, pour le champ **Machines sources**, sélectionnez l'objet réseau (machine, groupe de machines, plage d'adresses IP ou réseau) à l'origine du trafic devant être chiffré (LAN_Site_A dans l'exemple).
4. Dans le menu **Destination**, sélectionnez ou créez l'objet réseau (machine, groupe de machines, plage d'adresses IP ou réseau) destinataire du trafic chiffré (LAN_Site_B dans l'exemple).

5. Dans le menu **Port - Protocole**, sélectionnez le ou les ports correspondant aux protocoles devant être chiffrés (Any dans l'exemple).
6. Validez et appliquez le changement.

La règle de filtrage prend alors la forme suivante :

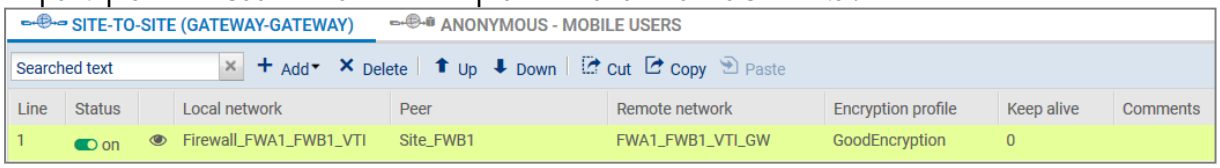


Mettre en œuvre la politique IPsec

Créez une politique VPN IPsec pour le chiffrement des flux traités par le firewall FWA1 (1/3 du trafic chiffré, le reste étant également réparti sur les routeurs FWA2 et FWA3).

1. Dans le module **Configuration** > **VPN** > **VPNIPsec**, sur l'onglet *Site à site (gateway-gateway)*, cliquez sur **Ajouter** et sélectionnez **Tunnel site à site**.
2. Créez un correspondant (IKEv1 ou IKEv2) avec les caractéristiques suivantes :
   - **Passerelle distante** : créez un objet portant l'adresse IP publique du firewall 1 du site B (FWB1 dans l'exemple),
   - **Nom** : laissez le nom proposé par défaut (Site_FWB1 dans l'exemple) ou personnalisez-le,
   - Sélectionnez le certificat à présenter ou indiquez une clé pré-partagée selon la méthode d'authentification choisie (pour plus de détails, consultez la documentation en ligne : *How to VPNIpSec - Authentification par clé prépartagée* et *How to VPN IPsec - Authentification par certificats*).
3. Dans le champ **Réseau local**, sélectionnez l'objet correspondant à l'interface virtuelle IPsec du firewall FWA1 (Firewall_FWA1_FWB1_VTI dans l'exemple).
4. Dans le champ **Réseau distant**, sélectionnez l'objet correspondant à l'interface virtuelle IPsec du firewall FWB1 (FWA1_FWB1_VTI_GW dans l'exemple).

La politique VPN IPsec du firewall FWA1 prendra donc la forme suivante :



Sauvegardez (bouton **Enregistrer**) et appliquez cette politique (bouton **Activer cette politique**).

Paramétrer le firewall FWA2

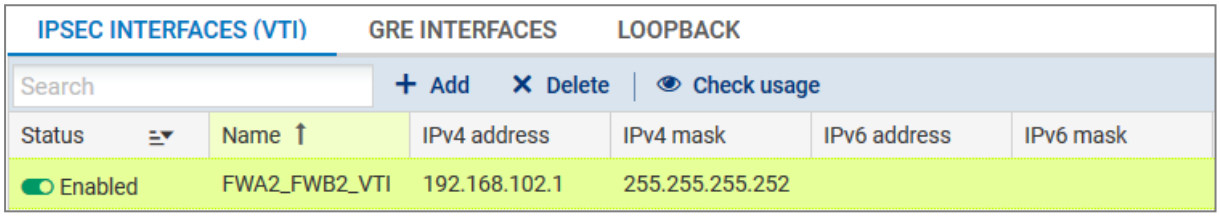
Le paramétrage de FWA2 consiste à :

- Créer une interface virtuelle IPsec,
- Définir une route vers le réseau distant,
- Définir les routes de retour,
- Mettre en œuvre la règle de filtrage,
- Mettre en œuvre la politique IPsec.

Créer une interface virtuelle IPsec

En suivant la méthode décrite pour le firewall FWA1, créez une interface IPsec virtuelle (VTI) sur laquelle sera basé le tunnel IPsec entre le firewall 2 du site A (FWA2) et le firewall 2 du site B (FWB2) :

- **Nom** : FWA2_FWB2_VTI dans l'exemple,
- **Adresse IP** : 192.168.102.1 dans l'exemple,
- **Masque** : 255.255.255.252 dans l'exemple.



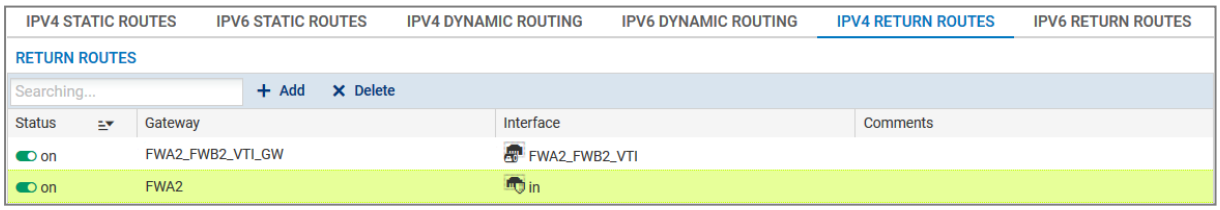
Définir une route vers le réseau distant

Bien que dans cette configuration le firewall effectue du routage au sein de la politique de filtrage (Policy Based Routing), il est **nécessaire de définir une route par défaut ou une route statique explicite vers le réseau distant**.

En effet, la première action effectuée par le firewall est de vérifier qu'il dispose d'une route vers le site distant avant de consulter sa politique de filtrage. L'absence de cette route provoquerait donc un rejet des paquets.

Définir les routes de retour

En suivant la méthode décrite pour le firewall FWA1, créez 2 routes permettant d'acheminer les paquets retour vers le firewall d'origine grâce à l'adresse MAC source.



Route de retour vers le firewall FWB2

- **Passerelle** : créez l'objet réseau correspondant à l'interface virtuelle IPsec du firewall 2 du site B (FWA2_FWB2_VTI_GW ayant pour adresse IP 192.168.102.2 dans l'exemple),
- **Interface** : sélectionnez l'interface virtuelle locale définie pour le tunnel IPsec entre les firewalls 2 des sites A et B (FWA2_FWB2_VTI dans l'exemple).

Activez la route par un double clic dans la colonne **État**.

Route de retour vers le firewall FWA1

- **Passerelle** : créez l'objet réseau correspondant au firewall 1 du site A (FWA1 dans l'exemple),

NOTE
L'adresse MAC du firewall FWA1 doit impérativement être déclarée dans cet objet réseau.

- **Interface** : sélectionnez l'interface du firewall FWA2 par laquelle les paquets retour seront acheminés vers le firewall FWA1 (In dans l'exemple).

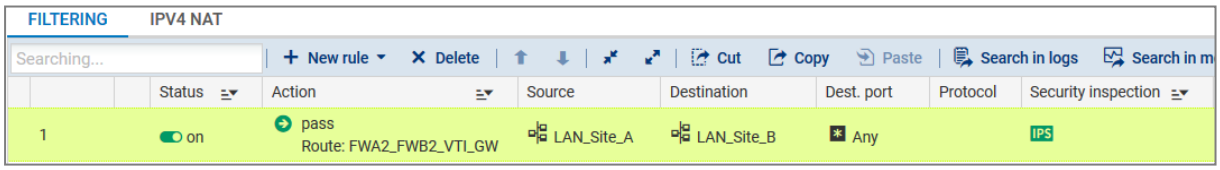
Activez la route par un double clic dans la colonne **État**.

Mettre en œuvre la règle de filtrage

Créez une règle de filtrage destinée à envoyer les flux chiffrés dans le tunnel basé sur l'interface virtuelle IPsec.

1. Dans le menu **Configuration** > **Politique de sécurité** > **Filtrage et NAT**, double-cliquez dans la colonne **État** pour le passer à **On**.
2. Dans la colonne **Action**, double-cliquez pour choisir la valeur *passer* pour le champ **Action**. Sélectionnez dans le champ **Passerelle - routeur** l'interface IPsec virtuelle du firewall 2 du site B (objet FWA2_FWB2_VTI_GW dans l'exemple).
3. Dans le menu **Source**, pour le champ **Machines sources**, sélectionnez le réseau à l'origine du trafic devant être chiffré (LAN_Site_A dans l'exemple).
4. Dans le menu **Destination**, sélectionnez ou créez l'objet réseau (machine, groupe de machines, plage d'adresses IP ou réseau) destinataire du trafic chiffré (LAN_Site_B dans l'exemple).
5. Dans le menu **Port - Protocole**, sélectionnez le ou les ports correspondant aux protocoles devant être chiffrés (Any dans l'exemple).

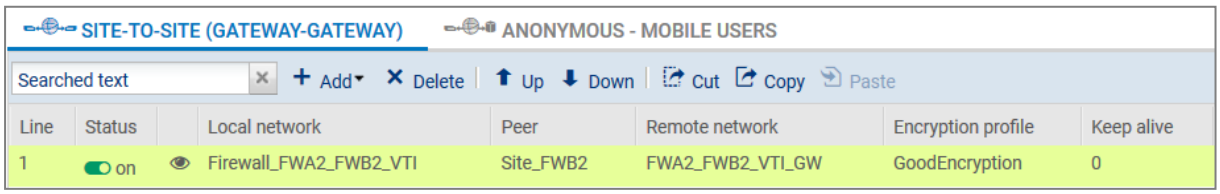
La règle de filtrage prend alors la forme suivante :



Mettre en œuvre la politique IPsec

En suivant la méthode décrite pour le firewall FWA1, créez une politique VPN IPsec pour le chiffrement des flux traités par le firewall FWA2 :

- **Correspondant** : créez un objet correspondant à l'adresse IP publique du firewall FWB2,
- **Réseau local** : sélectionnez l'objet correspondant à l'interface virtuelle IPsec locale (Firewall_FWA2_FWB2_VTI dans l'exemple),
- **Réseau distant** : sélectionnez l'objet correspondant à l'interface virtuelle IPsec distante (FWA2_FWB2_VTI_GW dans l'exemple).



Paramétrer le firewall FWA3

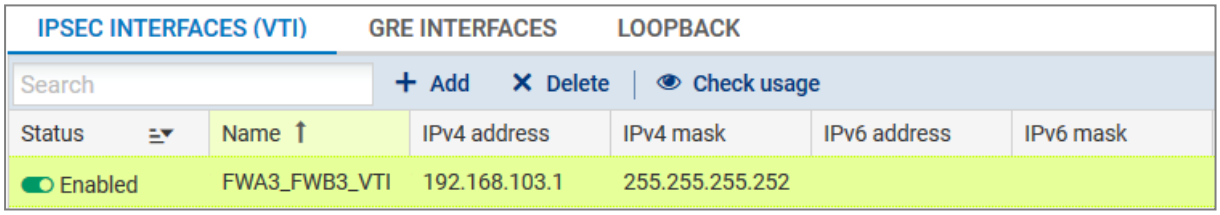
Le paramétrage de FWA3 consiste à :

- Créer une interface virtuelle IPsec,
- Définir une route vers le réseau distant,
- Définir les routes de retour,
- Mettre en œuvre la règle de filtrage,
- Mettre en œuvre la politique IPsec.

Créer une interface virtuelle IPsec

En suivant la méthode décrite pour le firewall FWA1, créez une interface IPsec virtuelle (VTI) sur laquelle sera basé le tunnel IPsec entre le firewall 3 du site A (FWA3) et le firewall 3 du site B (FWB3) :

- **Nom** : FWA3_FWB3_VTI dans l'exemple,
- **Adresse IP** : 192.168.103.1 dans l'exemple,
- **Masque** : 255.255.255.252 dans l'exemple.



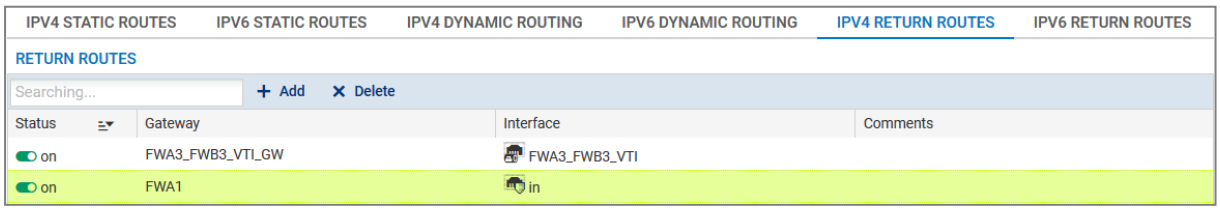
Définir une route vers le réseau distant

Bien que dans cette configuration le firewall effectue du routage au sein de la politique de filtrage (Policy Based Routing), il est **nécessaire de définir une route par défaut ou une route statique explicite vers le réseau distant**.

En effet, la première action effectuée par le firewall est de vérifier qu'il dispose d'une route vers le site distant avant de consulter sa politique de filtrage. L'absence de cette route provoquerait donc un rejet des paquets.

Définir les routes de retour

En suivant la méthode décrite pour le firewall FWA1, créez 2 routes permettant d'acheminer les paquets retour vers le firewall d'origine grâce à l'adresse MAC source.



Route de retour vers le firewall FWB3

- **Passerelle** : créez l'objet réseau correspondant à l'interface virtuelle IPsec du firewall 3 du site B (FWA3_FWB3_VTI_GW ayant pour adresse IP 192.168.103.2 dans l'exemple),
- **Interface** : sélectionnez l'interface virtuelle locale définie pour le tunnel IPsec entre les firewalls 3 des sites A et B (FWA3_FWB3_VTI dans l'exemple).

Activez la route par un double clic dans la colonne **État.**

Route de retour vers le firewall FWA1

- **Passerelle** : créez l'objet réseau correspondant au firewall 1 du site A (FWA1 dans l'exemple),

> **NOTE**
> L'adresse MAC du firewall FWA1 doit impérativement être déclarée dans cet objet réseau.

- **Interface** : sélectionnez l'interface du firewall FWA3 par laquelle les paquets retour seront acheminés vers le firewall FWA1 (In dans l'exemple).

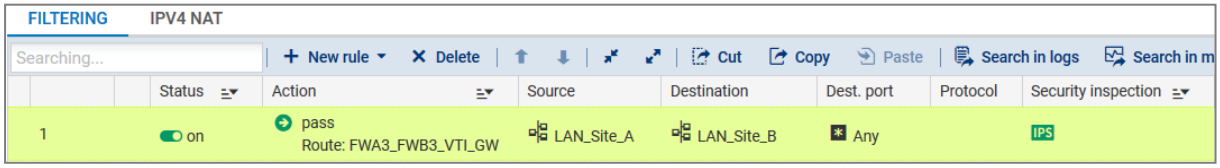
Activez la route par un double clic dans la colonne **État.**

Mettre en œuvre la règle de filtrage

Créez une règle de filtrage destinée à envoyer les flux chiffrés dans le tunnel basé sur l'interface virtuelle IPsec.

1. Dans le menu **Configuration** > **Politique de sécurité** > **Filtrage et NAT**, double-cliquez dans la colonne **État** pour le passer à **On**.
2. Dans la colonne **Action**, double-cliquez pour choisir la valeur *passer* pour le champ **Action**. Sélectionnez dans le champ **Passerelle - routeur** l'interface IPsec virtuelle du firewall 3 du site B (objet FWA3_FWB3_VTI_GW dans l'exemple).
3. Dans le menu **Source**, pour le champ **Machines sources**, sélectionnez le réseau à l'origine du trafic devant être chiffré (LAN_Site_A dans l'exemple).
4. Dans le menu **Destination**, sélectionnez ou créez l'objet réseau (machine, groupe de machines, plage d'adresses IP ou réseau) destinataire du trafic chiffré (LAN_Site_B dans l'exemple).
5. Dans le menu **Port - Protocole**, sélectionnez le ou les ports correspondant aux protocoles devant être chiffrés (Any dans l'exemple).

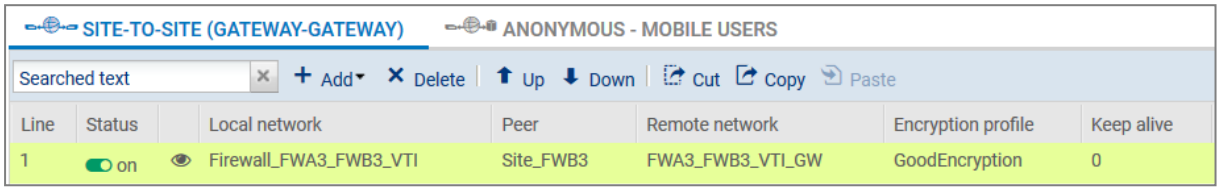
La règle de filtrage prend alors la forme suivante :



Mettre en œuvre la politique IPsec

En suivant la méthode décrite pour le firewall FWA1, créez une politique VPN IPsec pour le chiffrement des flux traités par le firewall FWA3 :

- **Correspondant** : créez un objet correspondant à l'adresse IP publique du firewall FWB3,
- **Réseau local** : sélectionnez l'objet correspondant à l'interface virtuelle IPsec locale (Firewall_FWA3_FWB3_VTI dans l'exemple),
- **Réseau distant** : l'objet correspondant à l'interface virtuelle IPsec distante(FWA3_FWB3_VTI_GW dans l'exemple).



Paramétrer le firewall FWB1

La configuration du firewall FWB1 est symétrique à celle réalisée pour le firewall FWA1.

En suivant la méthode décrite pour le firewall FWA1, procédez aux paramétrages suivants :

Créer une interface virtuelle IPsec

- **Nom** : FWB1_FWA1_VTI dans l'exemple,
- **Adresse IP** : 192.168.101.2 dans l'exemple,
- **Masque** : 255.255.255.252 dans l'exemple.

Définir une route vers le réseau distant

Bien que dans cette configuration le firewall effectue du routage au sein de la politique de filtrage (Policy Based Routing), il est **nécessaire de définir une route par défaut ou une route statique explicite vers le réseau distant**.

En effet, la première action effectuée par le firewall est de vérifier qu'il dispose d'une route vers le site distant avant de consulter sa politique de filtrage. L'absence de cette route provoquerait donc un rejet des paquets.

Définir les routes de retour

Route de retour vers le firewall FWA1

- **Passerelle** : créez un objet réseau en cliquant sur l'icône . Celui-ci doit correspondre à l'interface virtuelle IPsec du firewall 1 du site A (FWB1_FWA1_VTI_GW ayant pour adresse IP 192.168.101.1 dans l'exemple),
- **Interface** : sélectionnez l'interface virtuelle locale définie pour le tunnel IPsec entre les firewalls 1 des sites B et A (FWB1_FWA1_VTI dans l'exemple).

Activez la route par un double clic dans la colonne **État.**

Route de retour vers le firewall FWB2

- **Passerelle** : créez l'objet réseau correspondant au firewall 2 du site B (FWB2 dans l'exemple),

> **NOTE**
> L'adresse MAC du firewall FWB2 doit impérativement être déclarée dans cet objet réseau.

- **Interface** : sélectionnez l'interface du firewall FWB1 par laquelle les paquets retour seront acheminés vers le firewall FWB2 (Dmz1 dans l'exemple).

Activez la route par un double clic dans la colonne **État.**

Route de retour vers le firewall FWB3

- **Passerelle** : créez l'objet réseau correspondant au firewall 3 du site B (FWB3 dans l'exemple),

> **NOTE**
> L'adresse MAC du firewall FWB3 doit impérativement être déclarée dans cet objet réseau.

- **Interface** : sélectionnez l'interface du firewall FWB1 par laquelle les paquets retour seront acheminés vers le firewall FWB3 (Dmz2 dans l'exemple).

Activez la route par un double clic dans la colonne **État.**

Mettre en œuvre la règle de filtrage

- **Etat** : *On*,
- **Action**: *Passer*,
- **Machines sources** : LAN_Site_A dans l'exemple,
- **Machines destinations** : LAN_Site_B dans l'exemple,
- **Port destination** : Any dans l'exemple.

Mettre en œuvre la politique IPsec

- **Correspondant** : Site_FWA1 dans l'exemple,
- **Réseau local** : sélectionnez l'objet correspondant à l'interface virtuelle IPsec du firewall FWB1 (Firewall_FWB1_FWA1_VTI dans l'exemple),
- **Réseau distant** : sélectionnez l'objet correspondant à l'interface virtuelle IPsec du firewall FWA1 (FWB1_FWA1_VTI_GW dans l'exemple).

Paramétrer le firewall FWB2

La configuration du firewall FWB2 est symétrique à celle réalisée pour le firewall FWA2.

EEn suivant la méthode décrite pour le firewall FWA1, procédez aux paramétrages suivants :

Créer une interface virtuelle IPsec

- **Nom** : FWB2_FWA2_VTI dans l'exemple,
- **Adresse IP** : 192.168.102.2 dans l'exemple,
- **Masque** : 255.255.255.252 dans l'exemple.

Définir une route vers le réseau distant

Bien que dans cette configuration le firewall effectue du routage au sein de la politique de filtrage (Policy Based Routing), il est **nécessaire de définir une route par défaut ou une route statique explicite vers le réseau distant**.

En effet, la première action effectuée par le firewall est de vérifier qu'il dispose d'une route vers le site distant avant de consulter sa politique de filtrage. L'absence de cette route provoquerait donc un rejet des paquets.

Définir les routes de retour

En suivant la méthode décrite pour le firewall FWA1, créez 2 routes permettant d'acheminer les paquets retour vers le firewall d'origine grâce à l'adresse MAC source.

Route de retour vers le firewall FWA2

- **Passerelle** : créez l'objet réseau correspondant à l'interface virtuelle IPsec du firewall 2 du site A (FWB2_FWA2_VTI_GW ayant pour adresse IP 192.168.102.1 dans l'exemple),
- **Interface** : sélectionnez l'interface virtuelle locale définie pour le tunnel IPsec entre les firewalls 2 des sites B et A (FWB2_FWA2_VTI dans l'exemple).

Activez la route par un double clic dans la colonne **État.**

Route de retour vers le firewall FWB1

- **Passerelle** : créez l'objet réseau correspondant au firewall 1 du site B (FWB1 dans l'exemple),

> **NOTE**
> L'adresse MAC du firewall FWB1 doit impérativement être déclarée dans cet objet réseau.

- **Interface** : sélectionnez l'interface du firewall FWB2 par laquelle les paquets retour seront acheminés vers le firewall FWB1 (In dans l'exemple).

Activez la route par un double clic dans la colonne **État.**

Mettre en œuvre la règle de filtrage

- **Action** : *Passer*,
- **Machines sources** : LAN_Site_A dans l'exemple,
- **Machines destinations** : LAN_Site_B dans l'exemple,
- **Port destination** : Any dans l'exemple.

Mettre en œuvre la politique IPsec

- **Correspondant** : créez un objet correspondant à l'adresse IP publique du firewall FWA2,
- **Réseau local** : sélectionnez l'objet correspondant à l'interface virtuelle IPsec locale (Firewall_FWB2_FWA2_VTI dans l'exemple),
- **Réseau distant** : sélectionnez l'objet correspondant à l'interface virtuelle IPsec distante (FWB2_FWA2_VTI_GW dans l'exemple).

Paramétrer le firewall FWB3

La configuration du firewall FWB3 est symétrique à celle réalisée pour le firewall FWA3.

En suivant la méthode décrite pour le firewall FWA1, procédez aux paramétrages suivants :

Créer une interface virtuelle IPsec

- **Nom** : FWB3_FWA3_VTI dans l'exemple,
- **Adresse IP** : 192.168.103.2 dans l'exemple,
- **Masque** : 255.255.255.252 dans l'exemple.

Définir une route vers le réseau distant

Bien que dans cette configuration le firewall effectue du routage au sein de la politique de filtrage (Policy Based Routing), il est **nécessaire de définir une route par défaut ou une route statique explicite vers le réseau distant**.

En effet, la première action effectuée par le firewall est de vérifier qu'il dispose d'une route vers le site distant avant de consulter sa politique de filtrage. L'absence de cette route provoquerait donc un rejet des paquets.

Définir les routes de retour

Route de retour vers le firewall FWA3

- **Passerelle** : créez l'objet réseau correspondant à l'interface virtuelle IPsec du firewall 3 du site A (FWB3_FWA3_VTI_GW ayant pour adresse IP 192.168.103.1 dans l'exemple),
- **Interface** : sélectionnez l'interface virtuelle locale définie pour le tunnel IPsec entre les firewalls 3 des sites B et A (FWB3_FWA3_VTI dans l'exemple).

Activez la route par un double clic dans la colonne **État.**

Route de retour vers le firewall FWB1

- **Passerelle** : créez l'objet réseau correspondant au firewall 1 du site B (FWB1 dans l'exemple),

> **NOTE**
> L'adresse MAC du firewall FWB1 doit impérativement être déclarée dans cet objet réseau.

- **Interface** : sélectionnez l'interface du firewall FWB3 par laquelle les paquets retour seront acheminés vers le firewall FWB1 (In dans l'exemple).

Activez la route par un double clic dans la colonne **État.**

Mettre en œuvre la règle de filtrage

- **Action** : *Passer*,
- **Machines sources** : LAN_Site_A dans l'exemple,
- **Machines destinations** : LAN_Site_B dans l'exemple,

- **Port destination**: Any dans l'exemple.

Mettre en œuvre la politique IPsec

- **Correspondant** : créez un objet correspondant à l'adresse IP publique du firewall FWA3,
- **Réseau local** : sélectionnez l'objet correspondant à l'interface virtuelle IPsec locale (Firewall_FWB3_FWA3_VTI dans l'exemple),
- **Réseau distant** : l'objet correspondant à l'interface virtuelle IPsec distante(FWB3_FWA3_VTI_GW dans l'exemple).

Cas 2 : répartition de proxies

Paramétrer le Firewall FW1

Le paramétrage de FW1 consiste à :

- Définir une route vers le réseau distant,
- Définir les routes de retour,
- Définir la répartition de charge,
- Mettre en œuvre la règle de filtrage.

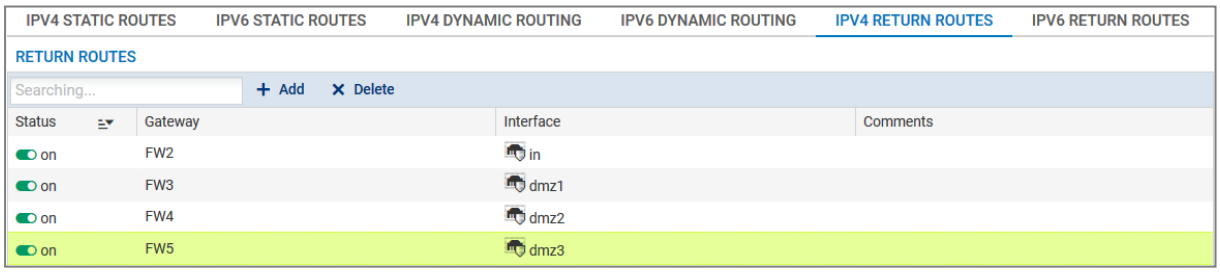
Définir une route vers le réseau distant

Bien que dans cette configuration le firewall effectue du routage au sein de la politique de filtrage (Policy Based Routing), il est **nécessaire de définir une route par défaut ou une route statique explicite vers le réseau distant**.

En effet, la première action effectuée par le firewall est de vérifier qu'il dispose d'une route vers le site distant avant de consulter sa politique de filtrage. L'absence de cette route provoquerait donc un rejet des paquets.

Définir les routes de retour

Créez 4 routes permettant d'acheminer les paquets retour vers le firewall d'origine grâce à son adresse MAC source :



Route de retour vers le firewall FW2

Dans le module **Configuration** > **Réseau** > **Routage**, sur l'onglet *Routes de retour*, cliquez sur le bouton **Ajouter**.

Renseignez les champs obligatoires :

- **Passerelle** : créez un objet réseau en cliquant sur l'icône . Celui-ci doit correspondre au firewall 2 du site (FW2 dans l'exemple),

> **NOTE**
> L'adresse MAC du firewall FW2 doit impérativement être déclarée dans cet objet réseau.

- **Interface** : sélectionnez l'interface du firewall FW1 par laquelle les paquets retour seront acheminés vers le firewall FW2 (interface in dans l'exemple).

Activez la route par un double clic dans la colonne **État.**

Route de retour vers le firewall FW3

- **Passerelle** : créez l'objet réseau correspondant au firewall 3 du site (FW3 dans l'exemple),

> **NOTE**
> L'adresse MAC du firewall FW3 doit impérativement être déclarée dans cet objet réseau.

- **Interface** : sélectionnez l'interface du firewall FW1 par laquelle les paquets retour seront acheminés vers le firewall FW3 (interface dmz1 dans l'exemple).

Activez la route par un double clic dans la colonne **État.**

Route de retour vers le firewall FW4

- **Passerelle** : créez l'objet réseau correspondant au firewall 4 du site (FW4 dans l'exemple),

> **NOTE**
> L'adresse MAC du firewall FW4 doit impérativement être déclarée dans cet objet réseau.

- **Interface** : sélectionnez l'interface du firewall FW1 par laquelle les paquets retour seront acheminés vers le firewall FW4 (interface dmz2 dans l'exemple).

Activez la route par un double clic dans la colonne **État.**

Route de retour vers le firewall FW5

- **Passerelle** : créez l'objet réseau correspondant au firewall 5 du site (FW5 dans l'exemple),

> **NOTE**
> L'adresse MAC du firewall FW5 doit impérativement être déclarée dans cet objet réseau.

- **Interface** : sélectionnez l'interface du firewall FW1 par laquelle les paquets retour seront acheminés vers le firewall FW5 (interface dmz3 dans l'exemple).

Activez la route par un double clic dans la colonne **État.**

Définir la répartition de charge

La répartition de charge des paquets à destination des deux firewalls ayant activé le proxy HTTP est réalisée grâce à un objet routeur composé des firewalls FW3 et FW4.

1. Dans le module **Configuration** > **Objets** > **Objets réseaux**, cliquez sur **Ajouter**.
2. Positionnez-vous sur le menu **Routeur**.
3. Indiquez un nom pour cet objet (HTTP_Proxy_LB dans l'exemple).
4. Dans l'onglet *Passerelles utilisées*, cliquez sur **Ajouter** et sélectionnez le firewall 3 du site (FW3). Laissez la valeur **Tester directement la passerelle** pour la colonne *Test de la disponibilité*. De même, laissez la valeur **1** dans la colonne *Poids*.
5. Répétez cette opération pour ajouter la passerelle FW4 :

6. Dans le panneau Configuration avancée, vérifiez que les différents champs prennent les valeurs suivantes :
   - **Répartition de charge**: *Par connexion* (chaque nouvelle connexion HTTP est envoyée vers l'une des deux passerelles déclarées selon le principe du Round-Robin),
   - **Activation des passerelles de secours**: *Lorsque toutes les passerelles sont injoignables*,
   - **Activer toutes les passerelles de secours en cas d'indisponibilité**: décochée,
   - **Si aucune passerelle n'est disponible**: *Routage par défaut*.
7. Validez la création de l'objet routeur en cliquant sur le bouton **Créer**.

Mettre en œuvre la règle de filtrage

Pour que les flux (HTTP, SSL, IMAP et POP3) soient dirigés vers les firewalls ayant activé le proxy adéquat, créez trois règles de filtrage intégrant une directive de routage :

- HTTPS vers le firewall FW2 pour solliciter son proxy SSL,
- HTTP vers l'objet HTTP_Proxy_LB pour répartir la charge entre les proxies HTTP des firewalls FW3 et FW4,
- SMTP/POP3/IMAP vers le firewall FW5 pour solliciter son proxy SMTP.

Les inspections de sécurité étant réalisées sur les firewalls ayant activé les différents proxies, les règles de sécurité du firewall FW1 pourront être en mode Firewall.

Flux HTTPS

1. Dans le menu **Configuration** > **Politique de sécurité** > **Filtrage et NAT**, double-cliquez dans la colonne **État** pour le passer à **On**.
2. Dans la colonne **Action**, double-cliquez pour choisir la valeur *passer* pour le champ **Action**. Sélectionnez dans le champ **Passerelle - routeur** l'objet correspondant au firewall ayant activé le proxy SSL (FW2 dans l'exemple).
3. Dans le menu **Source**, pour le champ **Machines sources**, sélectionnez le réseau à l'origine du trafic HTTPS (Network_bridge dans l'exemple).
4. Dans le menu **Destination**, sélectionnez l'objet *Internet*.
5. Dans le menu **Port - Protocole**, sélectionnez l'objet *https*.
6. Dans le menu **Inspection**, pour le champ **Niveau d'inspection**, sélectionnez le mode *Firewall*.
7. Validez la modification de la règle.

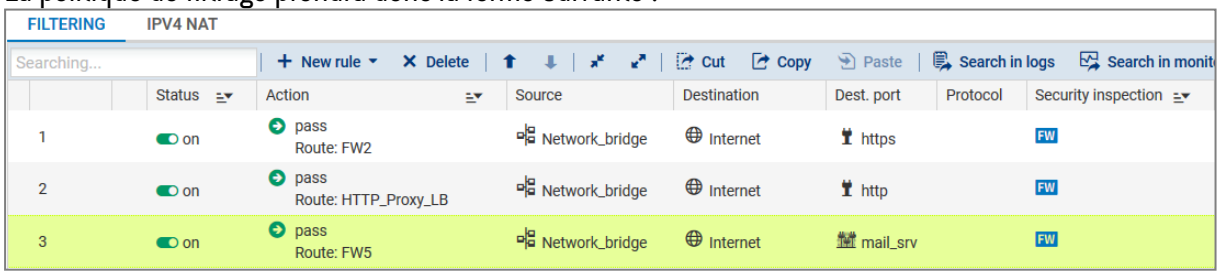
Flux HTTP

1. Ajoutez une nouvelle règle simple.
2. Double-cliquez dans la colonne **État** pour le passer à **On**.
3. Dans la colonne **Action**, double-cliquez pour choisir la valeur *passer* pour le champ **Action**. Sélectionnez dans le champ **Passerelle - routeur** l'objet routeur composé des deux firewalls FW3 et FW4 ayant activé le proxy HTTP (HTTP_Proxy_LB dans l'exemple).
4. Dans le menu **Source**, pour le champ **Machines sources**, sélectionnez le réseau à l'origine du trafic HTTP (Network_bridge dans l'exemple).
5. Dans le menu **Destination**, sélectionnez l'objet *Internet*.
6. Dans le menu **Port - Protocole**, sélectionnez l'objet *http*.
7. Dans le menu **Inspection**, pour le champ **Niveau d'inspection**, sélectionnez le mode *Firewall*.
8. Validez la modification de la règle.

Flux SMTP/IMAP/POP

1. Ajoutez une nouvelle règle simple.
2. Double-cliquez dans la colonne **État** pour le passer à **On**.
3. Dans la colonne **Action**, double-cliquez pour choisir la valeur *passer* pour le champ **Action**. Sélectionnez dans le champ **Passerelle - routeur** l'objet correspondant au firewall ayant activé le proxy SMTP (FW5 dans l'exemple).
4. Dans le menu **Source**, pour le champ **Machines sources**, sélectionnez le réseau à l'origine du trafic mail (Network_bridge dans l'exemple).
5. Dans le menu **Destination**, sélectionnez l'objet *Internet*.
6. Dans le menu **Port - Protocole**, sélectionnez l'objet *mail_srv* (cet objet couvre les 3 protocoles SMTP, IMAP et POP3).
7. Dans le menu **Inspection**, pour le champ **Niveau d'inspection**, sélectionnez le mode *Firewall*.
8. Validez la modification de la règle.

La politique de filtrage prendra donc la forme suivante :



Paramétrer le Firewall FW2

Le paramétrage de FW2 consiste à :

- Définir une route vers le réseau distant,
- Définir une route de retour,
- Activer le proxy SSL dans la règle de filtrage.

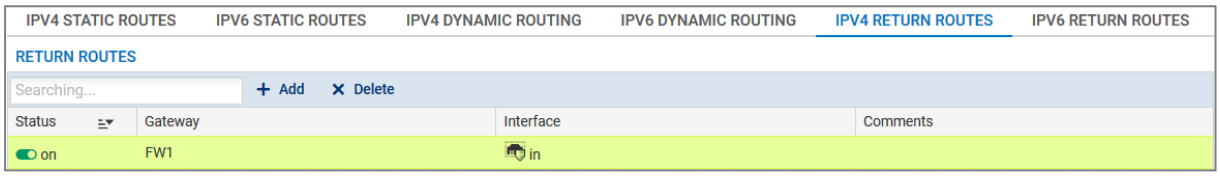
Définir une route vers le réseau distant

Il est **nécessaire de définir une route par défaut ou une route statique explicite vers le réseau distant**.

En effet, la première action effectuée par le firewall est de vérifier qu'il dispose d'une route vers le site distant avant de consulter sa politique de filtrage. L'absence de cette route provoquerait donc un rejet des paquets.

Définir une route de retour

Créez une route permettant d'acheminer les paquets retour vers le firewall d'origine grâce à son adresse MAC.



Route de retour vers le firewall FW1

- **Passerelle** : créez l'objet réseau correspondant au firewall 1 du site (FW1 dans l'exemple),

> **NOTE**
> L'adresse MAC du firewall FW1 doit impérativement être déclarée dans cet objet réseau.

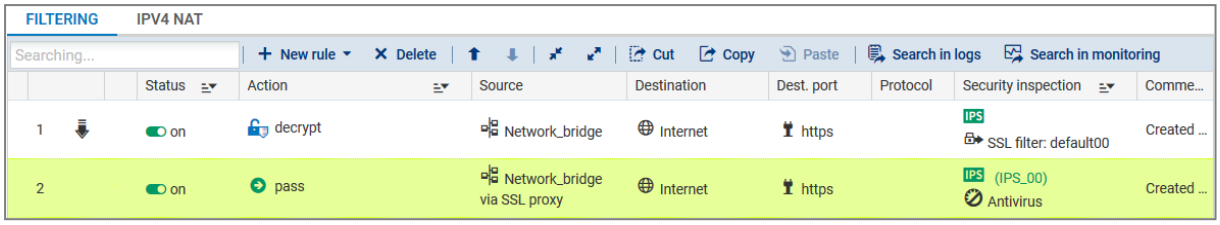
- **Interface** : sélectionnez l'interface du firewall FW2 par laquelle les paquets retour seront acheminés vers le firewall FW1 (interface in dans l'exemple).

Activez la route par un double clic dans la colonne **État.**

Activer le proxy SSL dans la règle de filtrage

1. Dans le menu **Configuration** > **Politique de sécurité** > **Filtrage et NAT**, ajoutez une nouvelle règle d'inspection SSL.
2. Dans le champ **Machines sources**, sélectionnez l'objet représentant les machines ou réseau à l'origine des flux HTTPS (objet Network_bridge dans l'exemple).
3. Dans le champ **Destination**, sélectionnez l'objet *Internet*.
4. Dans le champ **Port destination**, sélectionnez l'objet *https*.
5. Dans le champ **Profil d'inspection**, choisissez le profil d'inspection à appliquer (le choix Auto proposé par défaut applique le profil IPS_00 aux flux entrants et le profil IPS_01 aux flux sortants).
6. Dans le champ **Politique de filtrage SSL**, sélectionnez la politique de filtrage SSL à appliquer (default00 dans l'exemple).
7. Dans le champs **Antivirus**, activez l'antivirus en sélectionnant la valeur **On**.
8. Validez la modification de la règle.

La politique de filtrage prendra donc la forme suivante :



Paramétrer les Firewalls FW3 et FW4

Le paramétrage de FW3 et FW4 consiste à :

- Définir une route vers le réseau distant,
- Définir une route de retour,
- Activer le proxy HTTP dans la règle de filtrage.

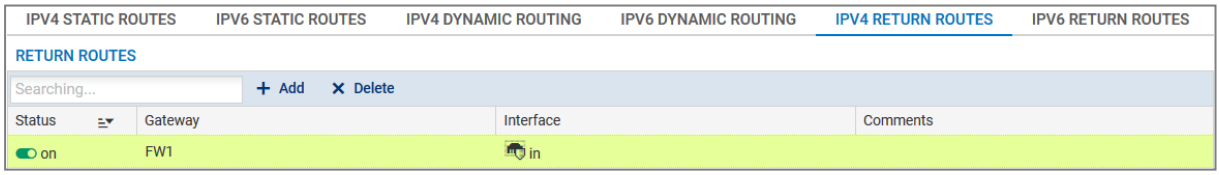
Définir une route vers le réseau distant

Il est **nécessaire de définir une route par défaut ou une route statique explicite vers le réseau distant**.

En effet, la première action effectuée par le firewall est de vérifier qu'il dispose d'une route vers le site distant avant de consulter sa politique de filtrage. L'absence de cette route provoquerait donc un rejet des paquets.

Définir une route de retour

Créez une route permettant d'acheminer les paquets retour vers le firewall d'origine grâce à son adresse MAC.



Route de retour vers le firewall FW1

Sur chacun des deux firewalls (FW3 et FW4), créez la route de retour suivante :

- **Passerelle** : créez l'objet réseau correspondant au firewall 1 du site (FW1 dans l'exemple),

> **NOTE**
> L'adresse MAC du firewall FW1 doit impérativement être déclarée dans cet objet réseau.

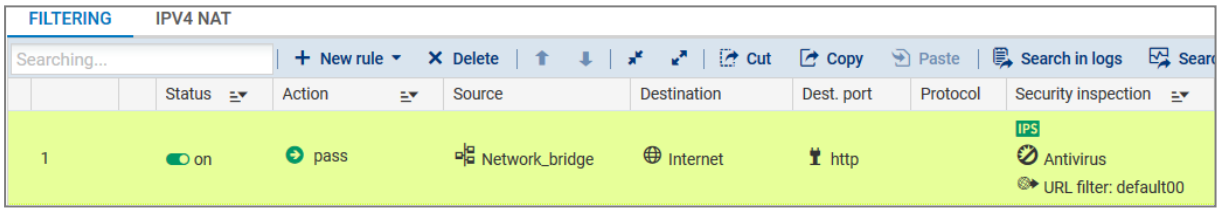
- **Interface** : sélectionnez l'interface du firewall FW3 (respectivement du firewall FW4) par laquelle les paquets retour seront acheminés vers le firewall FW1 (interface in dans l'exemple).

Activez la route par un double clic dans la colonne **État.**

Activer le proxy HTTP dans la règle de filtrage

1. Dans le menu **Configuration** > **Politique de sécurité** > **Filtrage et NAT**, ajoutez une nouvelle règle simple.
2. Double-cliquez dans la colonne **État** pour le passer à **On**.
3. Dans la colonne **Action**, double-cliquez pour choisir la valeur *passer* pour le champ **Action**.
4. Dans le menu **Source**, pour le champ **Machines sources**, sélectionnez le réseau à l'origine des flux de messagerie électronique (Network_bridge dans l'exemple).
5. Dans le menu **Destination**, sélectionnez l'objet *Internet*.
6. Dans le menu **Port - Protocole**, sélectionnez l'objet *http*.
7. Dans le menu **Inspection**, pour le champ **Profil d'inspection**, choisissez le profil d'inspection à appliquer (le choix Auto proposé par défaut applique le profil IPS_00 aux flux entrants et le profil IPS_01 aux flux sortants).
8. Toujours dans le menu **Inspection**, pour le champ **Antivirus**, sélectionnez la valeur **On**. Pour le champ **Filtrage d'URL**, sélectionnez la politique de filtrage d'URL à appliquer (default00 dans l'exemple).
9. Validez la modification de la règle.

La politique de filtrage prendra donc la forme suivante :



Paramétrer le Firewall FW5

Le paramétrage de FW5 consiste à :

- Définir une route vers le réseau distant,
- Définir une route de retour,
- Activer le proxy SMTP dans la règle de filtrage.

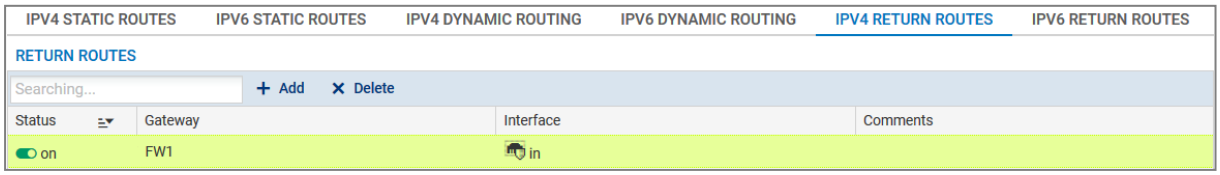
Définir une route vers le réseau distant

Il est **nécessaire de définir une route par défaut ou une route statique explicite vers le réseau distant**.

En effet, la première action effectuée par le firewall est de vérifier qu'il dispose d'une route vers le site distant avant de consulter sa politique de filtrage. L'absence de cette route provoquerait donc un rejet des paquets.

Définir une route de retour

Créez une route permettant d'acheminer les paquets retour vers le firewall d'origine grâce à son adresse MAC.



Route de retour vers le firewall FW1

- **Passerelle** : créez l'objet réseau correspondant au firewall 1 du site (FW1 dans l'exemple),

> **NOTE**
> L'adresse MAC du firewall FW1 doit impérativement être déclarée dans cet objet réseau.

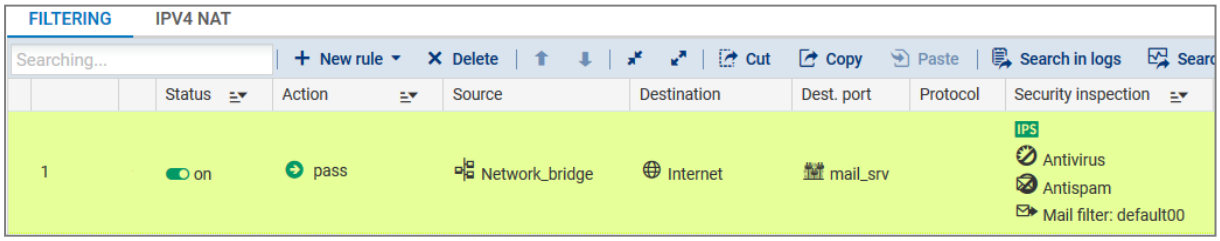
- **Interface** : sélectionnez l'interface du firewall FW2 par laquelle les paquets retour seront acheminés vers le firewall FW1 (interface in dans l'exemple).

Activez la route par un double clic dans la colonne **État.**

Activer le proxy SMTP dans la règle de filtrage

1. Dans le menu **Configuration** > **Politique de sécurité** > **Filtrage et NAT**, ajoutez une nouvelle règle simple.
2. Double-cliquez dans la colonne **État** pour le passer à **On**.
3. Dans la colonne **Action**, double-cliquez pour choisir la valeur *passer* pour le champ **Action**.
4. Dans le menu **Source**, pour le champ **Machines sources**, sélectionnez le réseau à l'origine des flux de messagerie électronique (Network_bridge dans l'exemple).
5. Dans le menu **Destination**, sélectionnez l'objet *Internet*.
6. Dans le menu **Port - Protocole**, sélectionnez l'objet *mail_srv* contenant les protocoles SMTP, IMAP et POP3.
7. Dans le menu **Inspection**, pour le champ **Profil d'inspection**, choisissez le profil d'inspection à appliquer (le choix Auto proposé par défaut applique le profil IPS_00 aux flux entrants et le profil IPS_01 aux flux sortants).
8. Toujours dans le menu **Inspection**, pour les champs **Antivirus** et **Antispam**, sélectionnez la valeur **On**. Pour le champ **Filtrage d'URL**, sélectionnez la politique de filtrage SMTP à appliquer (default00 dans l'exemple).
9. Validez la modification de la règle.

La politique de filtrage prendra donc la forme suivante :



Paramétrer le Firewall FW6

Le paramétrage de FW6 consiste à :

- Mettre en œuvre une règle de filtrage,
- Mettre en œuvre une règle de translation d'adresses (NAT).

Routes de retour

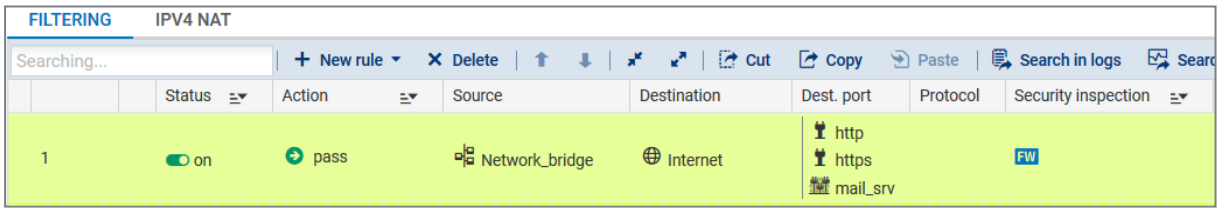
Il n'est pas nécessaire de définir des routes de retour sur ce firewall : les différents proxies activés sur les firewalls FW2 à FW5 (SSL, HTTP, SMTP/POP3/IMAP) réalisant par défaut de la translation d'adresses (case **Conserver l'adresse IP source originale** décochée dans le paramétrage de chacun de ces protocoles), le firewall FW6 connaît donc l'origine des paquets sources pour chacun de ces flux.

Mettre en œuvre une règle de filtrage

Créez une règle de filtrage autorisant les flux HTTP, HTTPS, SMTP, IMAP et POP3 à destination d'Internet. Les inspections de sécurité étant réalisées sur les firewalls ayant activé les différents proxies, la règle de sécurité du firewall FW6 pourra être en mode Firewall.

1. Dans le menu **Configuration** > **Politique de sécurité** > **Filtrage et NAT**, ajoutez une nouvelle règle simple.
2. Double-cliquez dans la colonne **État** pour le passer à **On**.
3. Dans la colonne **Action**, double-cliquez pour choisir la valeur *passer* pour le champ **Action**.
4. Dans le menu **Source**, pour le champ **Machines sources**, sélectionnez le réseau à l'origine du trafic (Network_bridge dans l'exemple).
5. Dans le menu **Destination**, sélectionnez l'objet *Internet*.
6. Dans le menu **Port - Protocole**, sélectionnez les objets *http*, *https* et *srv_mail*.
7. Dans le menu **Inspection**, pour le champ **Niveau d'inspection**, sélectionnez le mode *Firewall*.
8. Validez la modification de la règle.

La règle de filtrage prendra donc la forme suivante :



Mettre en œuvre une règle de translation d'adresses (NAT)

Créez une règle de NAT destinée à masquer les réseaux internes derrière l'adresse publique du firewall FW6.

1. Dans le menu **Configuration** > **Politique de sécurité** > **Filtrage et NAT**, positionnez-vous sur l'onglet *IPV4 NAT*.
2. Ajoutez une nouvelle règle simple.
3. Double-cliquez dans la colonne **État** pour le passer à **On**.
4. Dans la colonne **Source** du **Trafic original**, double-cliquez pour sélectionner le réseau à l'origine du trafic (Network_bridge dans l'exemple).
5. Dans le menu **Destination originale** sur l'onglet *Général*, pour le champ **Machines sources**, sélectionnez l'objet *Internet*. Pour le champ **Port destination**, sélectionnez l'*objet* Any.
6. Toujours dans le menu **Destination originale** sur l'onglet *Configuration avancée*, pour le champ **Interface de sortie**, sélectionnez l'interface de sortie vers Internet (interface *out* dans l'exemple).

7. Dans le menu **Source translatée**, pour le champ **Machine source translatée** , sélectionnez l'objet réseau correspondant à l'adresse publique du firewall FW6 (*Firewall_out* dans l'exemple). Pour le champ **Port source translaté**, choisissez l'objet **ephemeral_fw** et cochez la case **choisir aléatoirement le port source translaté**.
8. Dans le menu **Destination translatée**, pour le champ **Machine destination translatée** , laissez l'objet **Any** proposé par défaut.
9. Validez la modification de la règle.

La règle de NAT prendra donc la forme suivante :

		Original traffic (before translation)				Traffic after translation			
	Status	Source	Destination	Dest. port		Source	Src. port	Destination	Dest. port
1	on	Network_bridge	Internet interface: out	Any	→	Firewall_out	ephemeral	Any	

Pour aller plus loin

Base de connaissances Stormshield

Des informations complémentaires et réponses à vos éventuelles questions sont disponibles dans la base de connaissances Stormshield (authentification nécessaire).

documentation@stormshield.eu