Fiche savoirs technologiques : Mise en place du plan d'adressage réseau du Lab

Configuration des interfaces réseau

Dans une configuration usine :

- la **première interface** du pare-feu SNS est nommée **OUT** ou WAN,
- la seconde **IN**
- et le reste des interfaces **DMZx**.

L'interface « OUT » est une **interface externe** utilisée pour connecter le pare-feu SNS à internet (WAN) et le reste des interfaces sont internes et servent principalement à connecter le pare-feu SNS à des réseaux locaux.

La distinction interface interne/externe permet de se protéger contre les attaques d'usurpation d'adresse IP.

Pour accéder à l'interface d'administration du pare-feu SNS, il faut connecter votre machine sur une interface interne sous peine d'être détecté comme tentative d'intrusion qui nécessite le redémarrage du firewall.

Vous allez configurer votre pare-feu SNS selon les paramètres de l'architecture globale présentée dans l'activité précédente (interfaces IN, OUT et DMZ1) en utilisant le pare-feu SNS en mode **routeur**.

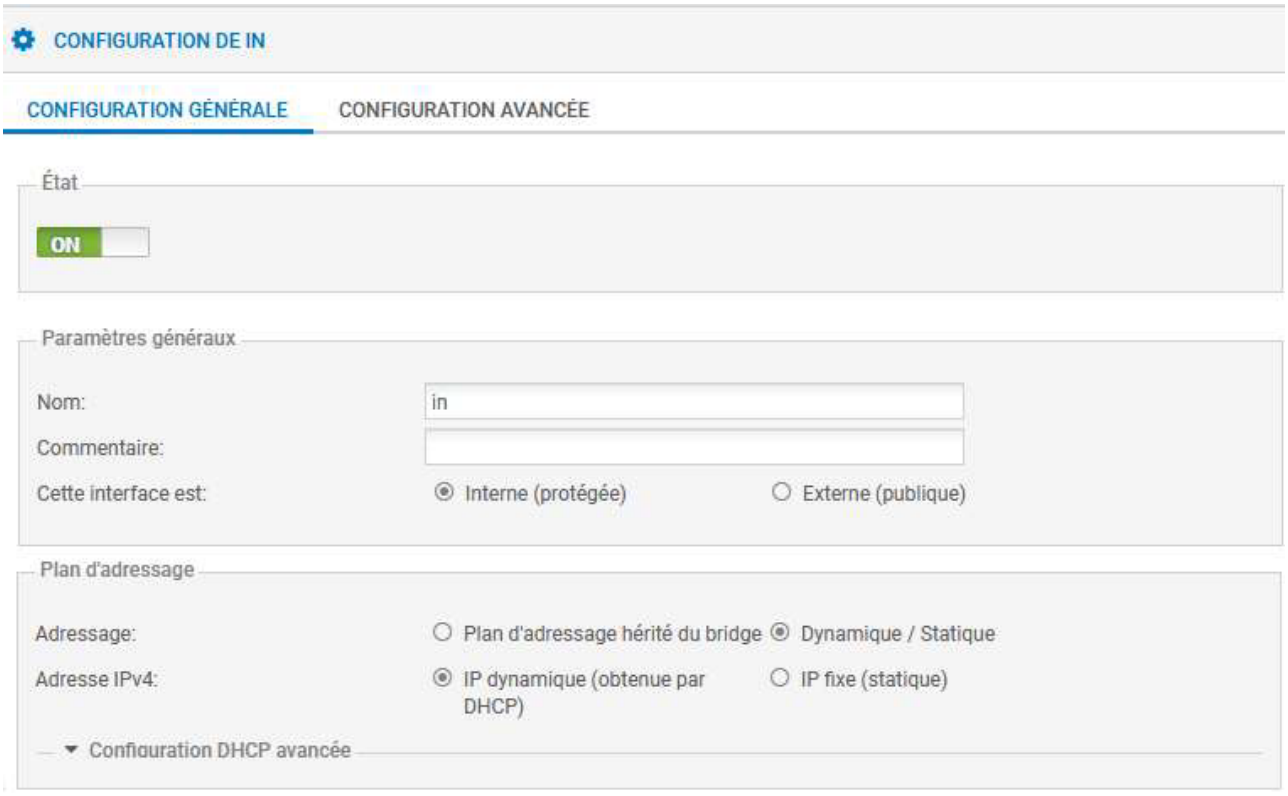
- @Interface **OUT** 192.36.253.x0 /24 qui correspond au premier port (WAN) ;
- @Interface **IN** 192.168.x.254 /24 qui correspond au deuxième port (port LAN N°1) ;
- @Interface **DMZ1** 172.16.x.254 /24 qui correspond au port DMZ.

La passerelle par défaut de votre pare-feu SNS est la passerelle du réseau NatNetwork de VirtualBox @192.36.253.1.

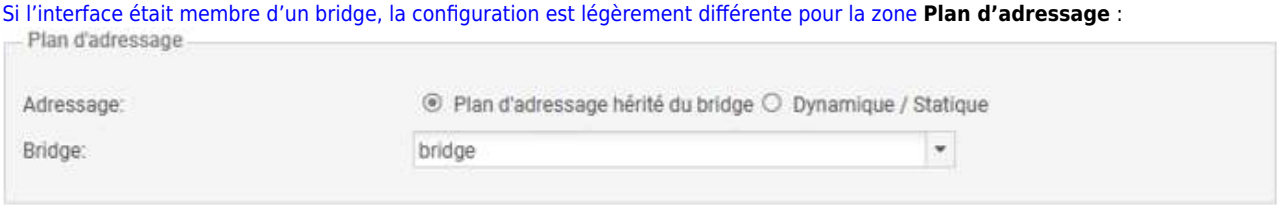
La configuration du SNS se fera depuis le client Linux Graphique connecté à l'interface **IN**.

La **configuration des interfaces** s'effectue dans le menu **Configuration** / **Réseau** / **Interfaces** en faisant sortir les interfaces Ethernet de l'interface bridge.

- Choisir une première interface (par exemple **IN**) pour la sortir du bridge ou la configurer avec une IP fixe ou dynamique (les manipulations sont identiques).



Si l'interface était membre d'un bridge, la configuration est légèrement différente pour la zone **Plan d'adressage** :



- Le cas échéant, cliquez dans la zone **Plan d'adressage** sur **Dynamique/Statique**
- Cliquez **Ip fixe (statique)**, un tableau apparaît :

- Cliquez sur **+Ajouter** et dans la zone Adresse / Masque saisissez **l'adresse IP de l'interface IN** 192.168.x.254 puis le masque en CIDR /24 ou en notation décimale pointée : 255.255.255.0

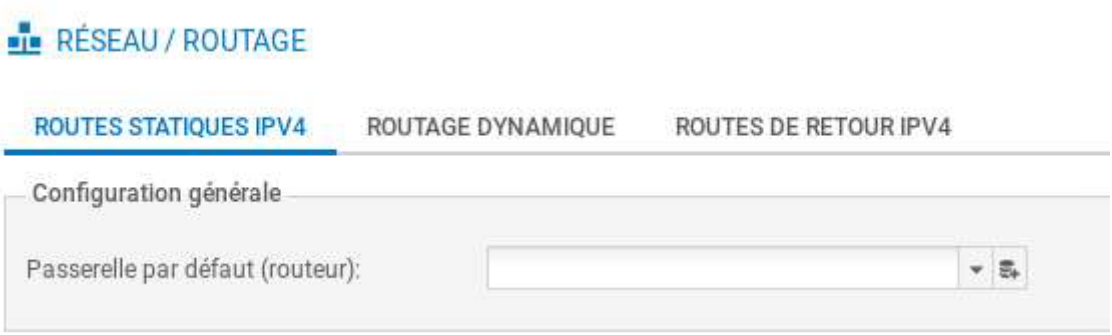
- Cliquez le bouton **Appliquer** puis **Sauvegarder** et à nouveau **Sauvegarder**. Un message de reconnexion peut s'afficher, le cas échéant reconnectez-vous.
- Procédez de manière identique pour les deux autres interfaces à configurer.

Route par défaut

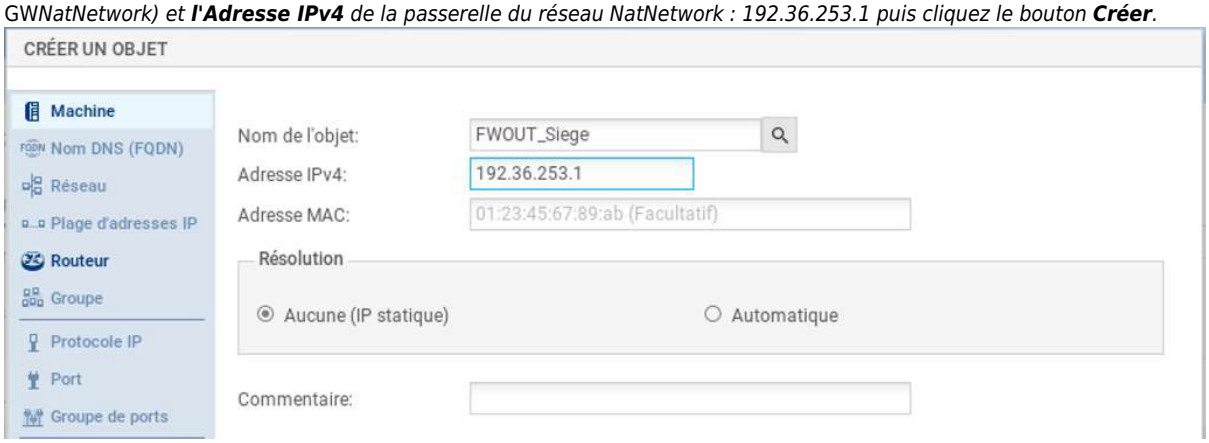
La configuration de la passerelle par défaut de votre pare-feu SNS doit pointer la passerelle du réseau NatNetwork de VirtualBox :

192.36.253.1

- Cliquez sur **Configuration** / **Réseau** / **Routage** onglet **Routes statiques IPv4** :



- Cliquez sur l'icône tout à droite pour **ajouter un objet réseau**, choisissez **Machine** et renseignez les champs **Nom** (Ex : GW*NatNetwork) et* ***l'Adresse IPv4*** *de la passerelle du réseau NatNetwork : 192.36.253.1 puis cliquez le bouton* ***Créer****.*



===== Mise en oeuvre de la traduction d'adresses pour l'accès à Internet (NAT/PAT) ===== Pour le LAB, nous considérons le réseau externe inter-entreprises comme un réseau public dans lequel aucune adresse IP privée n'est tolérée. De plus, la passerelle du réseau NatNetWork est connecté à internet via une interface autre que celles utilisées dans l'architecture du LAB. * Ouvrez le menu **Configuration** / **Politique de sécurité** / **Filtrage et NAT.** :

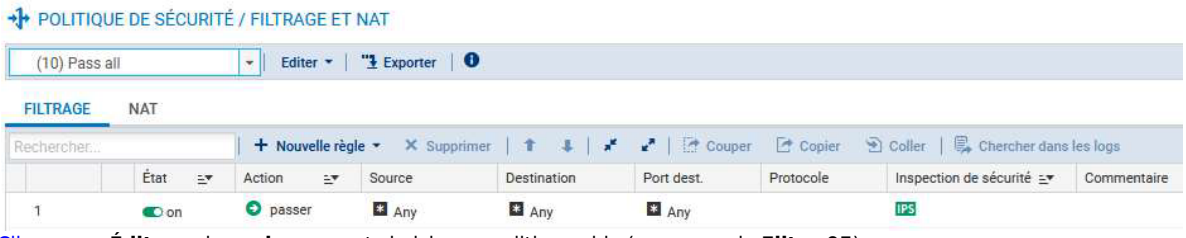
Dans les pare-feux SNS, les règles de filtrage et de NAT (traduction d'adresses) sont regroupées sous une même politique. Il est possible de définir 10 politiques différentes mais une seule politique est active à la fois, identifiée par une icône. La politique de sécurité active en configuration usine est **(1) Block all** : elle n'autorise que le ping des interfaces du firewall et l'accès en https à l'administration du boitier. Une politique implicite **Block all** est également configurée sur le pare-feu SNS.

Pour réaliser les activités, vous allez choisir une politique plus permissive que vous durcirez progressivement.

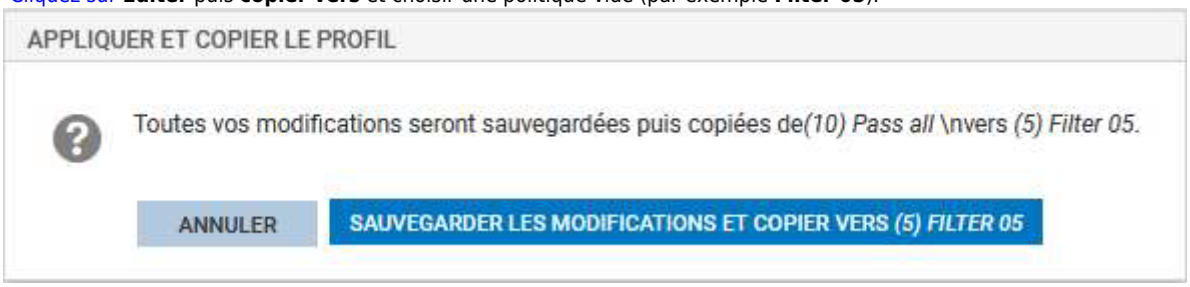
Étape 1 :

- Copiez la politique de filtrage/NAT **(10) Pass all** vers une autre politique vide en la renommant **AgenceX** (remplacez X par la lettre de votre entreprise).
- Ensuite, **activez cette politique**.

* Dans la liste déroulante des politiques de sécurité, choisissez (10) Pass all. Cette politique laisse explicitement passer tous les flux.



* Cliquez sur **Éditer** puis **copier vers** et choisir une politique vide (par exemple **Filter 05**).



===== Retour Accueil Stormshield ===== * Stormshield