NOTE TECHNIQUE

STORMSHIELD NETWORK SECURITY

METTRE EN ŒUVRE UNE RÈGLE DE NAT

Produits concernés : SNS 1 et versions supérieures

Date : 19 juin 2019

Référence : sns-fr-mettre_en_oeuvre_regle-NAT_Note_Technique

Table des matières

Mettre en œuvre une règle de NAT

Le mécanisme de translation d'adresses (Network Address Translation - NAT) a été mis au point afin de répondre à la pénurie d'adresses IP. En effet, l'adressage IPv4 ne dispose pas d'un nombre suffisant d'adresses IP routables, donc uniques, pour connecter l'ensemble des machines à internet.

Des plages d'adresses IP privées (10.0.0.0/8, 172.16.0.0/12 et 192.168.0.0/16) ont donc été réservées pour les usages internes. Le mécanisme de NAT permet ainsi de connecter l'ensemble de ces réseaux privés à Internet.

IMPORTANT

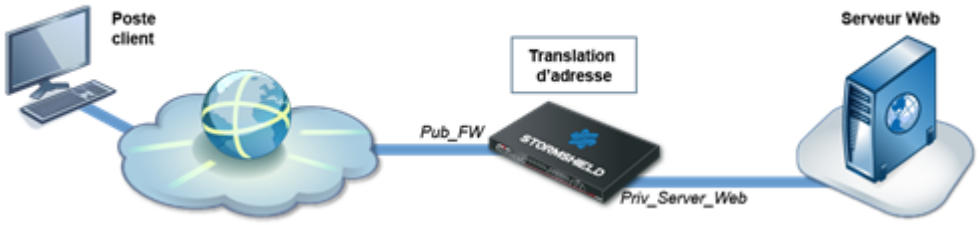
La politique de filtrage est appliquée au trafic avant sa modification par le NAT.

Objectif

Vous souhaitez autoriser les accès en HTTP depuis les machines externes vers votre serveur Web au travers de votre Firewall Stormshield Network.

Votre entreprise ne dispose que d'une seule adresse IP publique. Votre serveur sera donc visible depuis l'extérieur au travers de cette unique adresse publique portée par l'IPS-Firewall.

On parle de translation statique de type "1 adresse IP publique pour n adresses IP privées" (sur des ports différents).



Créer les objets réseau

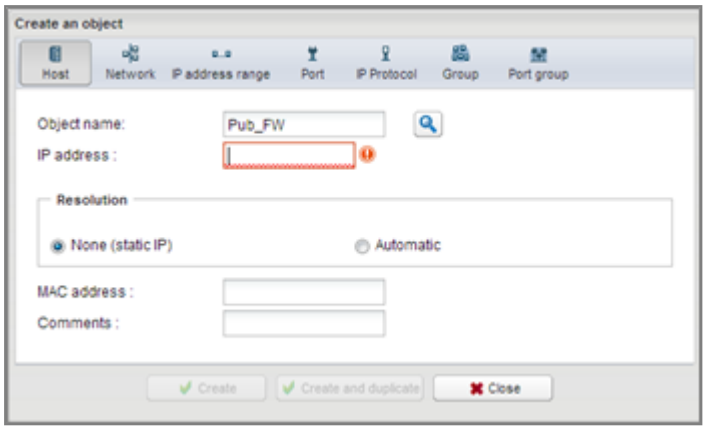
Pour réaliser cette configuration, deux objets réseau seront nécessaires :

- l'adresse privée du serveur web. Exemple : **Priv_Webserver**,
- l'adresse publique de l'IPS-Firewall. Exemple : **Pub_FW**.

Dans le menu **Configuration** > **Objets** > **Objets réseau** :

1. Cliquez sur **Ajouter** pour créer ces objets.
2. Vérifiez que l'onglet **Machine** est bien sélectionné.

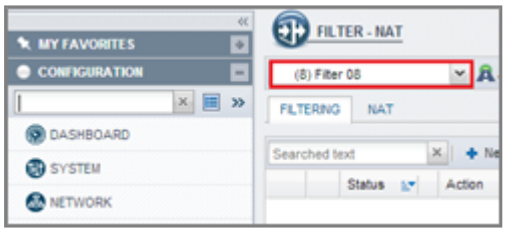
3. Renseignez les champs **Nom de l'objet** et **Adresse IP**



4. Cliquez sur **Créer et dupliquer** pour définir les différents objets réseau.
5. Lorsque le dernier objet a été défini, terminez l'opération en cliquant sur **Créer**.

Sélectionner la politique de filtrage / NAT

1. Cliquez sur **Configuration** > **Politique de Sécurité** > **Filtrage et NAT**.
2. Choisissez la politique de filtrage à modifier:

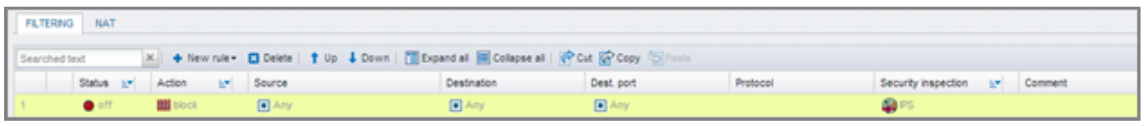


3. Vous pouvez renommer cette politique en cliquant sur **Éditer** > **Renommer.**

Créer la règle de filtrage et de NAT

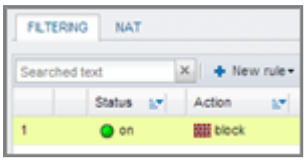
Le Firewall bloquant par défaut tout trafic non explicitement autorisé, il convient donc de créer une règle de filtrage acceptant le flux HTTP depuis Internet vers votre serveur Web. Les règles de NAT pourront directement être précisées au sein de cette règle de filtrage.

Dans l'onglet **Filtrage**, cliquez sur **Nouvelle règle** > **Règle standard**. Une nouvelle règle, inactive par défaut, est créée :



État

Faites un double clic sur la valeur off de la colonne **État**.
L'état de la règle change et passe à **on** :



Action

1. Faites un double clic sur **Bloquer** dans la colonne **Action**.
2. Pour le champ **Action**, choisissez **passer**,
3. Pour le champ **Niveau de trace**, vous pouvez choisir tracer si vous souhaitez que les flux correspondant à cette règle soient visibles dans les traces de filtrage du Firewall.

Source

1. Faites un double clic sur la valeur **Any** de la colonne **Source**.
2. Dans le champ **Machines sources**, sélectionnez l'objet réseau **Internet**.

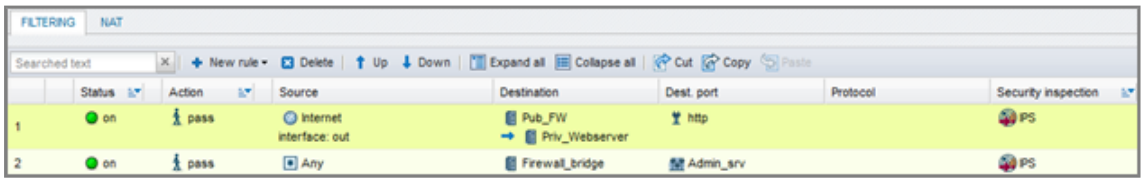
Destination

1. Faites un double clic sur la valeur **Any** de la colonne **Destination.**
2. Dans le champ **Machines destinations** de l'onglet **Général**, choisissez votre objet réseau **Pub_FW.**

Port destination

1. Faites un double clic sur la valeur **Any** de la colonne **Port dest.**
2. Pour le champ **Port destination**, sélectionnez **HTTP**.

La règle de filtrage et de NAT prend donc la forme suivante:



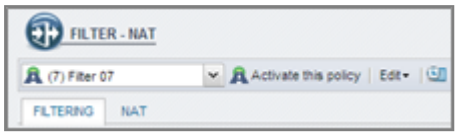
NOTE

Il est bien sûr possible de compléter cette règle à l'aide des fonctionnalités étendues des Firewalls Stormshield Network (Profils d'inspection de sécurité personnalisés, programmation horaire, etc.).

Activer la politique de filtrage

1. Au bas de la fenêtre **Filtrage et NAT**, cliquez sur **Sauvegarder et activer**.
2. Confirmez en cliquant sur **Activer la politique**.

3. La politique active est repérée grâce au symbole :



Tester la politique de filtrage / NAT

La procédure est terminée ; votre serveur web doit être accessible depuis un poste client externe: dans un navigateur web, indiquez l'URL du serveur, par exemple, « http://Adresse_Publique_Fw ».

Si la page d'accueil du serveur intranet ne s'affiche pas, vérifiez les points suivants :

- Votre politique de Filtrage/NAT et les règles associées sont-elles bien actives ?
- Le routage entre le poste client et le serveur est-il bien défini (routes statiques, passerelle par défaut vers l'IPS-Firewall) ?
- Le service web est-il bien démarré sur le serveur
- Existe-t-il un firewall bloquant la connexion sur le poste ou le serveur ?

STORMSHIELD

documentation@stormshield.eu