NOTE TECHNIQUE

STORMSHIELD NETWORK SECURITY

METTRE EN ŒUVRE UNE RÈGLE DE FILTRAGE

Produits concernés : SNS 3.x, SNS 4.x

Dernière mise à jour du document : 9 décembre 2019

Référence : sns-fr-mettre_en_oeuvre_regle-filtrage_Note_Technique

Table des matières

Avant de commencer

Vous souhaitez autoriser les accès en HTTP depuis un poste du réseau interne vers un serveur intranet (situé sur une DMZ par exemple) au travers de votre Firewall Stormshield Network.

NOTE
Pour une connexion à un autre type de serveur applicatif, comme un serveur de bases de données par exemple, la procédure est la même à l'exception de la valeur du ou des port(s) de destination.

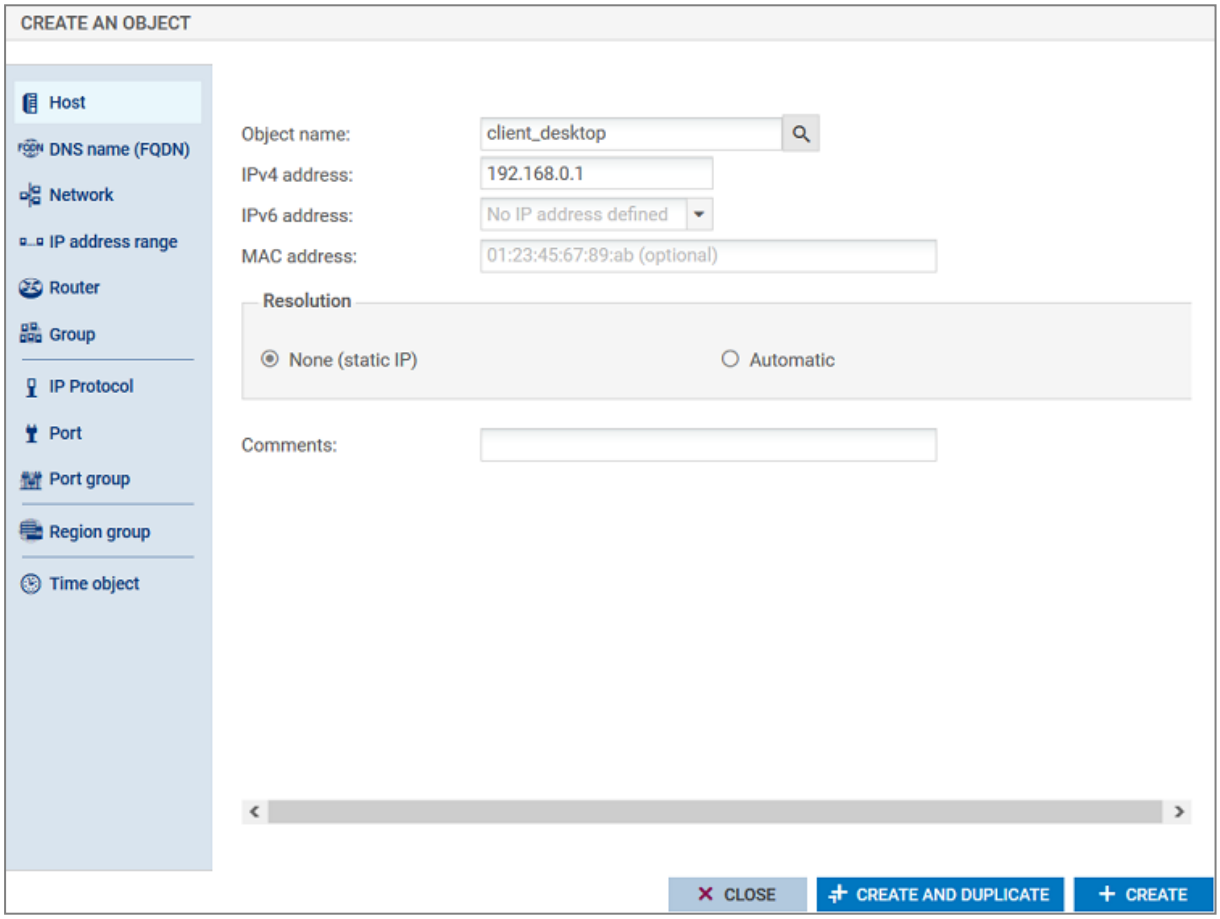
Prérequis

Le poste client et le serveur intranet doivent pouvoir dialoguer :

- soit en ayant le Firewall comme passerelle par défaut,
- soit grâce à une route statique via le Firewall.

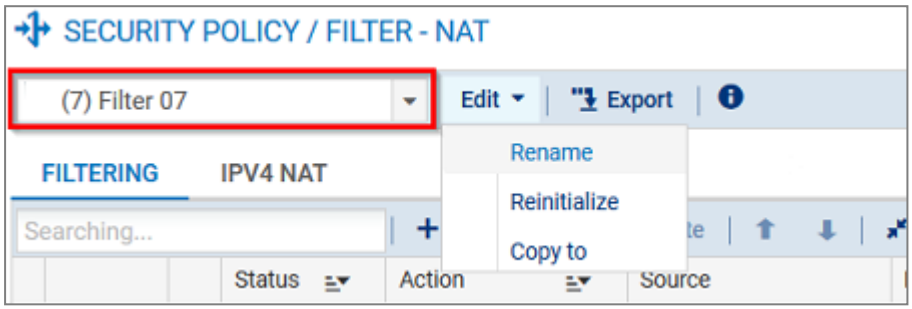
Créer les objets réseau

1. Dans le module **Configuration** > **Objets** > **Objets réseau**, cliquez sur **Ajouter**.
2. Dans l'assistant, vérifiez que l'onglet **Machine** est bien sélectionné.
3. Renseignez les champs **Nom de l'objet** et **Adresse IP** pour le poste client (objet **client_desktop**),
4. Validez par **Créer** et **dupliquer** afin de poursuivre par la création de l'objet **intranet_server** sur le même modèle.
5. Lorsque le dernier objet a été défini, terminez l'opération en cliquant sur **Créer**.
   Cette création d'objets réseau peut également être réalisée lors de l'élaboration de la politique de filtrage (étapes de sélection des sources et destinations).



Sélectionner une politique de filtrage

1. Positionnez-vous sur le module **Configuration** > **Politique de Sécurité** > **Filtrage et NAT**.
2. Choisissez la politique de filtrage à modifier.
3. Vous pouvez la renommer en cliquant sur **Éditer** > **Renommer**.



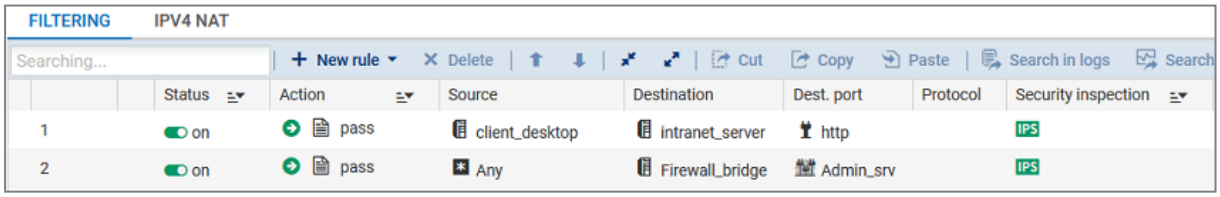
Ajouter une règle de filtrage

1. Dans le module **Configuration** > **Politique de sécurité** > **Filtrage et NAT**, cliquez sur **Nouvelle règle** > **Règle standard**.
2. Double-cliquez dans la colonne **État** pour passer la valeur à **On**.
3. Dans la colonne **Action**, double-cliquez pour choisir la valeur *passer* pour le champ **Action**. 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.
4. Dans le menu **Source**, pour le champ **Machines sources**, sélectionnez votre objet réseau **client_desktop**. Vous pouvez affiner votre règle de filtrage en précisant une **Interface d'entrée** sur laquelle le réseau de votre poste client est relié.
5. Dans le menu **Destination**, pour le champ **Machines sources**, sélectionnez votre objet réseau **intranet_server**. Depuis l'onglet *Configuration Avancée*, vous pouvez affiner votre règle de filtrage en précisant une **Interface de sortie** sur laquelle le serveur intranet est rattaché.
6. Dans le menu **Port - Protocole**, sélectionnez l'objet *http*.
7. Validez la modification de la règle.

Règle pour administrer le Firewall

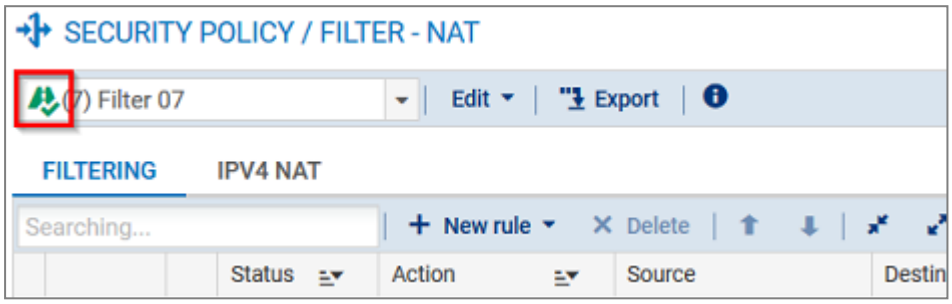
En suivant la même méthode, ajoutez une règle autorisant l'administration du Firewall en utilisant ces valeurs :

- Source : **Any** (ou un groupe de machines autorisées),
- Destination : l'objet **Firewall_Bridge**,
- Port : l'objet **Admin_Srv**.



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 désormais repérée grâce à un symbole.



Tester la politique de filtrage

La procédure est terminée. Votre intranet doit être accessible depuis votre poste client : dans un navigateur web, indiquez l'URL du serveur, par exemple, http://adresse_IP_serveur_intranet/.

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

- Votre politique de filtrage 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 le Firewall) ?
- Le service web est-il bien démarré sur le serveur ?
- Existe-t-il un firewall logiciel bloquant la connexion sur le poste ou le serveur ?

Pour aller plus loin

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

documentation@stormshield.eu