Mise en place de Par-feu et configuration des règles de filtrage

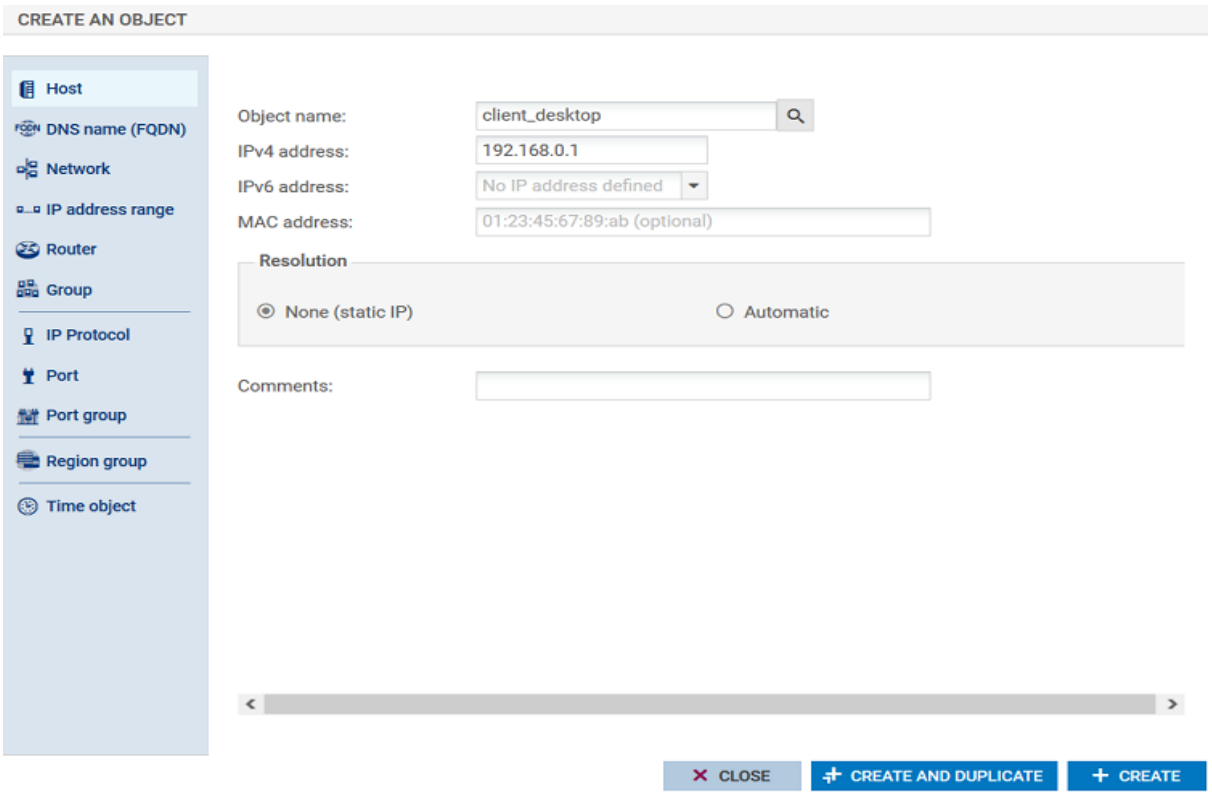
Créer les objets réseau

Afin de créer des objets réseau, rendez-vous dans le module **Configuration > Objets > Objets réseau**, cliquez sur **Ajouter**.

Puis dans l'assistant, vérifiez que l'onglet Machine est bien sélectionné et renseignez les champs **Nom de l'objet** et **Adresse IP** pour le poste client (objet client_desktop).

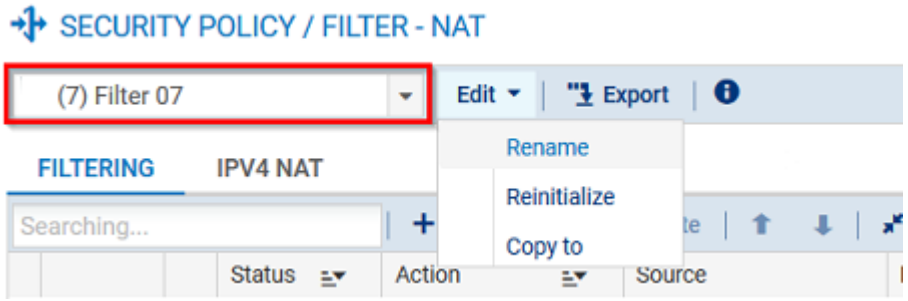
Enfin, validez par **Créer et dupliquer** afin de poursuivre par la création de l'objet **intranet_server** sur le même modèle.

Lorsque le dernier objet a été défini, terminez l'opération en cliquant sur **Créer**.
La 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

Pour ce faire, positionnez-vous sur le module **Configuration > Politique de Sécurité > Filtrage et NAT** puis choisissez la politique de filtrage à modifier.
Vous pouvez la renommer en cliquant sur **Éditer > Renommer.**



Ajouter une règle de filtrage

Rendez-vous dans l'onglet **Configuration > Politique de sécurité > Filtrage et NAT**, cliquez sur **Nouvelle règle > Règle standard**.

Double-cliquez dans la colonne **État** pour passer la valeur à **On** puis 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.

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.

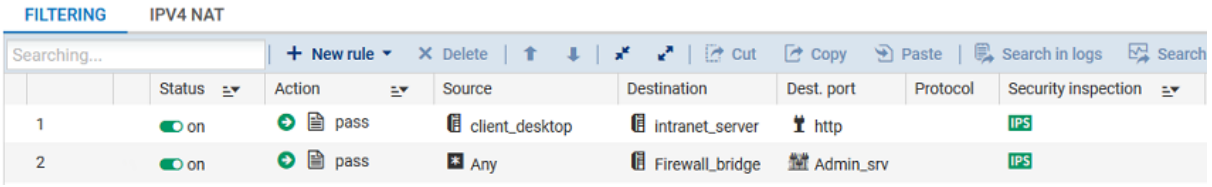
Puis dans le menu Destination, pour le champ **Machines sources**, sélectionnez votre objet **réseau intranet_server**. Depuis l'onglet Configuration Avancée, vous pouvez affiner votre règle de filtrage en précisant une Interface de sortie sur laquelle le serveur intranet est rattaché.

Dans le menu **Port - Protocole**, sélectionnez l'objet **http** Puis validez la modification de la règle.

Règle pour administrer le Firewall

Avec la méthode vu précédemment, vous pouvez ajoutez une règle autorisant l'administration du Firewall en utilisant ces valeurs :

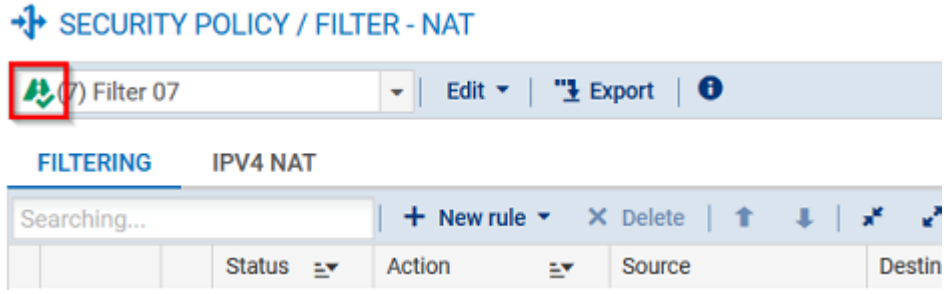
- Source : Any (ou un groupe de machines autorisées),
- Destination : l'objet Firewall_Bridge,
- Port : l'objet Admin_Srv.



Activer la politique de filtrage

En bas de la fenêtre Filtrage et NAT, cliquez sur **Sauvegarder et activer**, puis confirmez en cliquant sur **Activer la politique**.

La politique active est désormais repérée grâce à un symbole.



Tester la politique de filtrage

Afin de tester la politique de filtrage, rendez vous dans un navigateur web et indiquez l'URL du serveur, par exemple, http://IP_serveur_intranet

Dans mon cas le test est concluant, j'arrive bien à accéder au serveur intranet.