Fiche savoirs technologiques 4 : Configuration du NAT/PAT

Dans cette partie, vous allez reprendre l'architecture présentée dans la fiche N°1 et mettre en place des règles de NAT qui vont permettre d'accéder aux serveurs en DMZ de l'autre agence à travers des IP **publiques**.

Dans la fiche 2 vous avez mis en place une règle de NAT pour permettre l'accès à Internet à vos réseaux internes via la passerelle de l'enseignant.

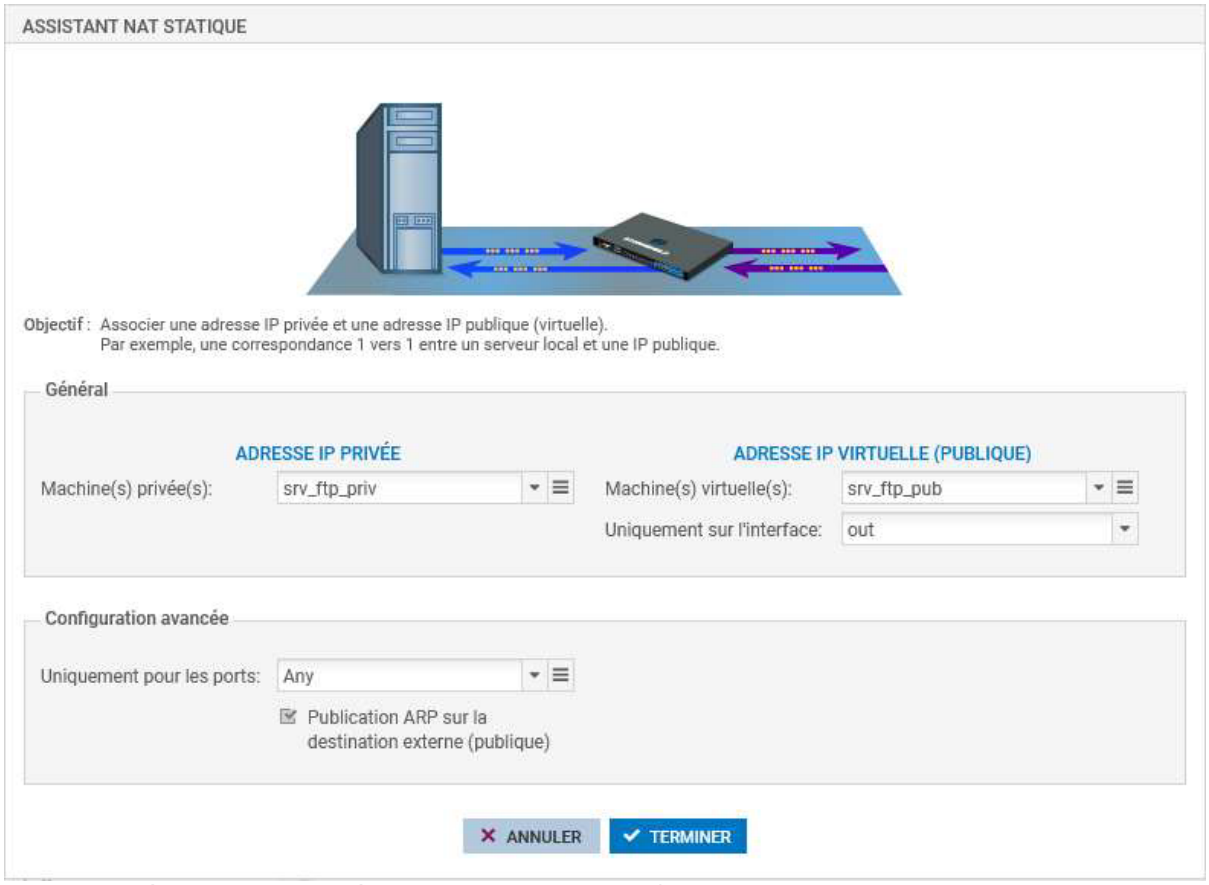
Vous allez maintenant configurer des règles de NAT et des règles de redirections de ports afin de rendre accessible vos services hébergés par le serveur Debian de la DMZ.

Mise en oeuvre de la NAT statique

Vous disposez de 2 adresses IP publiques **192.36.253.x2** et **192.36.253.x3** réservées respectivement à vos serveurs FTP et MAIL (au besoin ajoutez ces 2 objets créés cf Partie 3).

> **Étape 1 :** Vous allez ajouter les règles de NAT qui permettent de joindre chaque serveur depuis le réseau externe grâce à son adresse IP publique.

- Dans votre politique **AgenceX**, sélectionnez l'onglet **NAT** puis **Nouvelle règle/ règle de NAT statique (bimap)** ; un assistant s'ouvre :
    - **Machine(s) privée(s)** : L'adresse IP privée du serveur en interne
        - **Machine(s) virtuelle(s)** : L'adresse IP publique virtuelle dédiée au serveur interne
        - **Uniquement sur l'interface** : L'interface externe depuis laquelle le serveur est accessible avec son adresse IP publique virtuelle.
        - **Uniquement pour les ports** : La règle de NAT statique permet de translater tous les ports. Cependant, il est possible de la restreindre en spécifiant un ou une plage de ports au niveau de ce paramètre. Il est conseillé de laisser cette valeur à **Any** et de restreindre le port directement dans les règles de filtrage.
        - **publication ARP** : cochez **Activer la publication ARP** pour l'adresse IP publique.



- Dans **Adresse IP Privée, Machine(s) privée(s)**, choisissez l'adresse privée de la machine FTP : objet **srv*ftp*priv**.
- Dans **Adresse IP Virtuelle, Machine(s) virtuelle (s)**, choisissez l'adresse publique de la machine FTP : objet **srv*ftp*pub**.

- Choisissez **out** dans **Uniquement sur l'interface** et laissez **Any** dans **Uniquement pour les ports** et cochez **Publication ARP**
  - et cliquez **Terminer**.

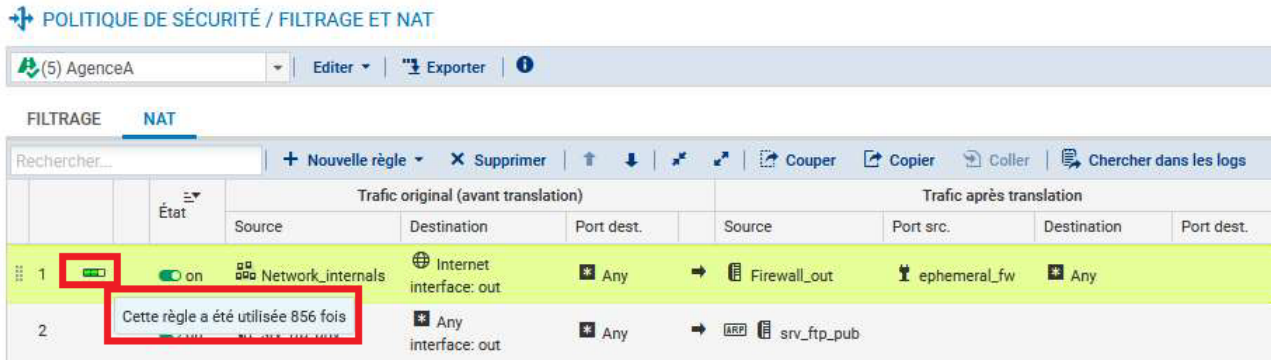
L'assistant **ajoute deux règles NATs** :

- La première règle pour la translation du **flux sortant** du serveur interne vers le **réseau public**
- et la **deuxième** pour le **flux entrant** à destination de l'adresse **IP publique virtuelle**. Les deux règles peuvent être modifiées par la suite indépendamment l'une de l'autre.

- Procédez de manière identique pour le serveur mail : objet **srv*mail*priv** et objet **srv*mail*pub**

Étape 2 : Testez l'application de la première règle de NAT, en envoyant un ping vers la passerelle par défaut.

- Envoyez un ping vers la passerelle par défaut de **l'autre agence** depuis la machine serveur debian du réseau de votre agence (AgenceX) ;
- Ouvrez **Configuration / Politique de sécurité / Filtrage et NAT** onglet **NAT** sur le firewall de votre agence (AgenceX). Dans la liste des règles la barre devient **verte** quand les règles **s'appliquent** et une info-bulle indique le nombre de fois où la règle a été appliquée :



Dans le bandeau d'affichage des règles, dépliez le menu (3 traits horizontaux) et cliquez sur **Réinitialiser les statistiques des règles** pour remettre les compteurs à zéro.

Mise en oeuvre de la redirection de ports

Étape 3 : Vous allez ajouter une **règle de NAT** afin que votre serveur **WEB** (objet srv*web*pub, protocole http) soit joignable grâce à une redirection de port via l'adresse IP publique OUT de votre firewall : **192.36.253.x0**.

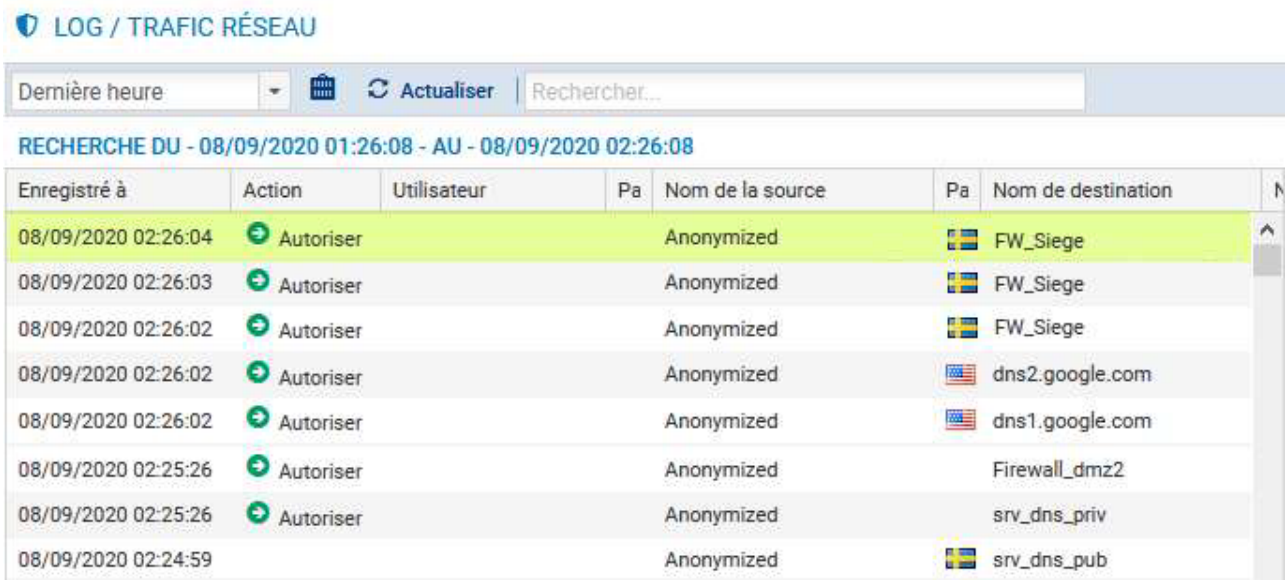
- Dans votre politique **AgenceX**, sélectionnez l'onglet **NAT** puis **Nouvelle règle / règle simple** et modifiez avec les paramètres suivants :
- Source originale = **Internet**,
- Interface d'entrée = **out**,
- Destination originale = **Firewall*Out*, * *Port dest= http*, * *Source translatée = Any*, * *Destination translatée = srvwebpriv*, * *Port destination translaté = ephemeralfw*.**

===== Traçage des règles de NAT =====

Étape 4 : Vous allez activez le **traçage des règles de NAT** pour les **flux entrants**, ceci permet d'avoir les informations visibles dans les **Journaux d'audit (logs)**.

* Double-cliquez une règle (par ex la règle n°3), et choisissez l'onglet **Options**, et dans niveau de trace **tracer* puis OK. * Répétez l'opération pour les autres règles entrantes.**

Vous pouvez tester l'accès à l'ensemble de vos ressources et vérifiez le traçage des règles demandées (flux entrants) dans les logs du firewall. Vous pouvez par exemple tenter d'accéder via des ping d'une machine debian à l'autre. * Cliquez l'onglet **Monitoring** puis **LOGS - Journaux d'audit / Vues / Trafic réseau** : vous devriez voir apparaître les ping vers la passerelle du Siège effectués précédemment.



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