

Fiche 6 – Configuration du NAT/PAT

Table des matières

I Mise en œuvre du NAT dynamique.....	1
II Mise en œuvre du NAT statique par port (redirection de port).....	4

Dans les pare-feu SNS, les règles de filtrage et 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 l'icône : 

I Mise en œuvre du NAT dynamique

La règle de NAT dynamique **NAPT** permet aux machines du réseau interne (**Network_internals**) d'accéder au réseau externe (**Network_Out**) et à Internet

La règle de **NAT dynamique** est créée avec le bouton **Nouvelle règle / règle de partage d'adresse source (masquerading)** qui ajoute automatiquement la plage de ports prédéfinie **ephemeral_fw** [20000-59999] au niveau du port source dans le trafic après traduction. Par défaut, les ports sont choisis séquentiellement dans cette plage, cependant une option est disponible pour permettre un choix aléatoire du numéro de port pour chaque nouvelle connexion et le rendre ainsi moins prédictible.

- Dans votre politique (**10**), sélectionner l'onglet **NAT** puis **Nouvelle règle / règle de partage d'adresse source (masquerading)**

FILTRE

NAT

Rechercher...

+ Nouvelle règle X Supprimer

Couper

Copier

Coller

Chercher dans les logs

	État	Trafic original (avant translation)			Trafic après translation				Protocole	Options
		Source	Destinat...	Port dest.	Source	Port src.	Destination	Port d...		
1	<div><div></div>off</div>	<div>Any</div>	<div>Any</div>	<div>Any</div>	<div>Any</div>	<div>ephemeral_fw</div>	<div>Any</div>			

Une nouvelle règle non activée apparaît avec des valeurs par défaut any, any. Dans la section **Trafic après translation**, le port source sera traduit par un numéro de port choisi dans la plage **ephemeral_fw**.

La configuration du **Trafic original (avant translation)** permet de renseigner les valeurs des paramètres avant traduction (par défaut any, any) :

- **Source** permet de définir l'adresse IP d'un hôte ou du réseau source ;
- **Destination** permet de définir l'adresse IP d'un hôte ou du réseau destination.

La configuration du **Trafic après translation** permet de renseigner les nouvelles valeurs des paramètres après traduction (par défaut any, any) :

- **Source** définit l'adresse IP ou le réseau source et le **port** source vus de l'extérieur.
- **Destination** définit l'adresse IP ou le réseau destination et **Port destination** traduite le port de destination.

Pour configurer un NAT/PAT pour permettre la sortie sur Internet

- Double-cliquer sur une zone vide de la règle pour ouvrir la fenêtre de configuration détaillée « **Edition de la règle N°1** ».
- Cliquer l'onglet du menu de gauche **Général**, dans la zone **Commentaire**, saisir un commentaire, par exemple « Configuration de la règle de NAT/PAT pour la sortie internet ».
- Cliquer sur l'onglet du menu de gauche **Source Originale**.
- Double-cliquer sur Any et avec la flèche choisir **Network_internals** (qui renvoie à tous les réseaux internes protégés), dans l'onglet Configuration avancée, laissez **Any** pour le port de destination.

EDITION DE LA RÈGLE N° 1

Général	SOURCE AVANT TRANSLATION (ORIGINALE)
Source originale	GÉNÉRAL CONFIGURATION AVANCÉE
Destination originale	Général
Source tradatée	Utilisateur: [Rechercher...]
Destination tradatée	Machines sources: [Ajouter] [Supprimer] [Network_internals]
Protocole	
Options	

- Cliquer sur l'onglet du menu de gauche **Destination originale**.
- Double-cliquer sur **Any** et avec la flèche choisir **Internet**, laissez **Any** pour le port de destination.

EDITION DE LA RÈGLE N° 1

Général	DESTINATION AVANT TRANSLATION (ORIGINALE)
Source originale	GÉNÉRAL CONFIGURATION AVANCÉE
Destination originale	Général
Source tradatée	Machines destinations: [Ajouter] [Supprimer] [Internet]
Destination tradatée	Port destination: [Ajouter] [Supprimer] [Any]
Protocole	
Options	



Attention : si dans la zone **destination originale**, vous laissez **Any**, plutôt qu'**Internet** qui désigne tous les réseaux sauf ceux internes au pare-feu SNS, le pare-feu SNS bloquera les flux d'administration (en ssh et en https). En effet, les flux d'administration subiront également une traduction NAT vers l'interface **OUT** qui l'interprétera comme une tentative d'intrusion et les bloquera.



Vous pouvez rendre cette règle plus restrictive en choisissant explicitement l'interface de sortie.

- Cliquer sur l'onglet **Configuration avancée** et sélectionnez **out** dans **Interface de sortie**.

EDITION DE LA RÈGLE N° 1

Général	DESTINATION AVANT TRANSLATION (ORIGINALE)
Source originale	GÉNÉRAL CONFIGURATION AVANCÉE
Destination originale	Configuration avancée
Source tradatée	Interface de sortie: [out]
Destination tradatée	<input type="checkbox"/> Publication ARP sur la destination externe (publique)
Protocole	
Options	

- Cliquer sur l'onglet **Source tradatée** et sélectionner **Firewall_Out** dans **Machine source tradatée**.
- Dans **Port source tradaté**, laissez **ephemeral_fw** et cocher **choisir aléatoirement le port source tradaté**.



Cette option **choisit aléatoirement le port source traduit**, ce qui permet d'éviter les attaques utilisant la prédictibilité des ports utilisés. Ainsi si le premier port est 20000, le suivant ne sera pas 20001. Cette précaution n'empêche pas les attaques, elle permet de les rendre plus complexes.

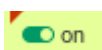
- Cliquer l'onglet du menu de gauche **Protocole**, cela permet de définir le type de protocole : applicatif, IP ou Ethernet, laisser **Détection automatique du protocole (par défaut)**

- Cliquer sur l'onglet du menu de gauche **Options**, cela permet de tracer le trafic qui correspond à la règle de traduction dans le journal de connexions, choisir **tracer**.

NB : Le journal de connexion permet de relever les opérations liées au NAT à l'aide des mot-clés « modsrc » et « modsrcport » en ligne de commande et « Adresse source traduite », « Port source traduit » via l'interface web d'administration. L'option « tracer » est utilisée à des fins de diagnostic afin de suivre le premier paquet passant dans la règle de NAT concernée.

- Cliquer sur **OK** pour sauvegarder les modifications de la règle de NAT dynamique que vous venez de créer.
- Dans la colonne **État**, sélectionner avec la flèche **Définir l'état on**

La règle passe à

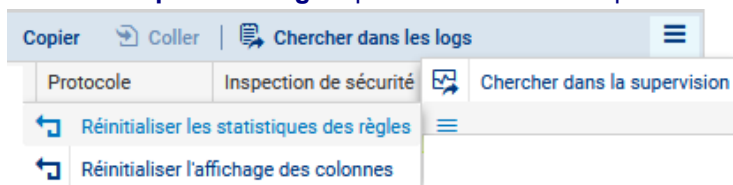


☑️ Cliquer sur **Appliquer** puis **Oui, Activer la politique** puis confirmer.

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 :

FILTRE NAT									
Rechercher...									
+ Nouvelle règle - X Supprimer [icône] [icône] [icône] [icône] Couper Copier Colier Chercher dans les logs									
	État	Trafic original (avant translation)			Trafic après translation				
		Source	Destination	Port dest.	Source	Port src.	Destination	Port dest.	
1	on	Network_Internals	Internet interface: out	Any	FirewallOut	ephemeral_fw	Any		
Cette règle a été utilisée 12 fois									

☑️ Dans le bandeau d'affichage des règles, déplier le menu ☰ et cliquer sur **Réinitialiser les statistiques des règles** pour remettre les compteurs à zéro.



II Mise en œuvre du NAT statique par port (redirection de port)

Pour faire une redirection NAT « classique », il faut sélectionner l'onglet **NAT** puis **Nouvelle règle / règle simple**.

Exemple avec une règle de NAT afin qu'un serveur WEB (objet `srv_web_priv`, protocole `http`) soit joignable grâce à une redirection de port via l'adresse IP publique OUT d'un pare-feu: « 192.36.253.70 ».

Source originale = **Internet**, Interface d'entrée = **out**

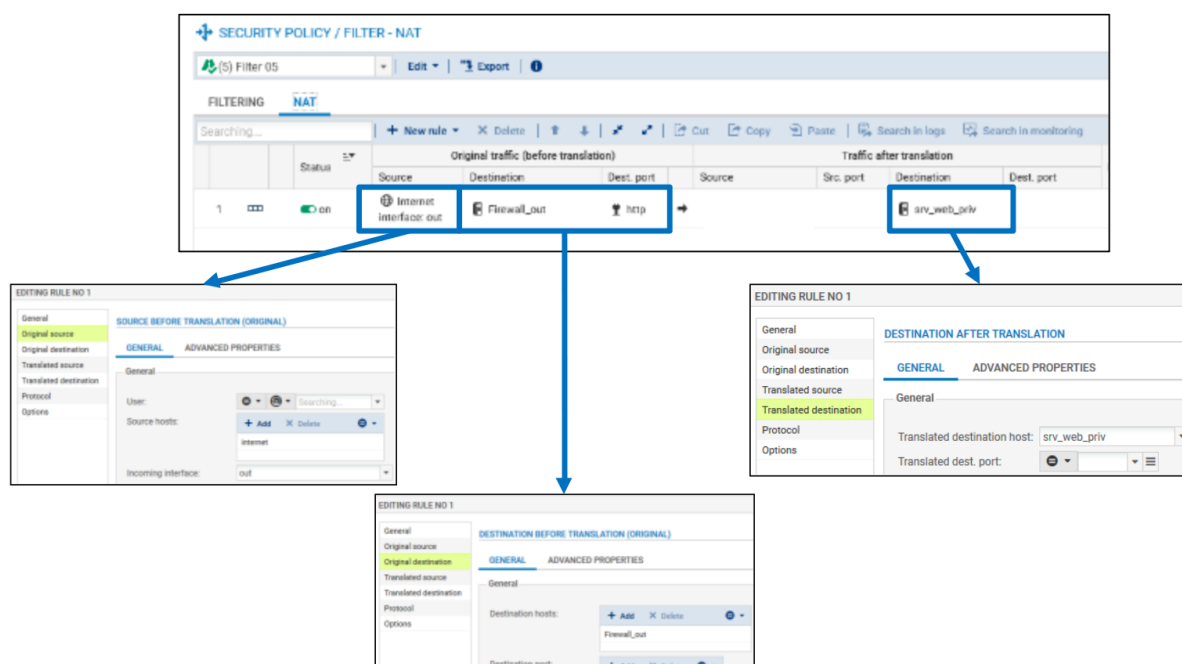
Destination originale = **Firewall_Out**, Port dest= **http**

Source tradatée = **Any** (ou pas de source), Destination tradatée = **srv_web_priv**, Port destination tradatée = **none**

6	on	Internet interface: out	Firewall_out	http	Any	srv_web_priv
---	----	-------------------------	--------------	------	-----	--------------

☑️ Cliquer **Appliquer** puis **Oui, Activer la politique** puis confirmer.

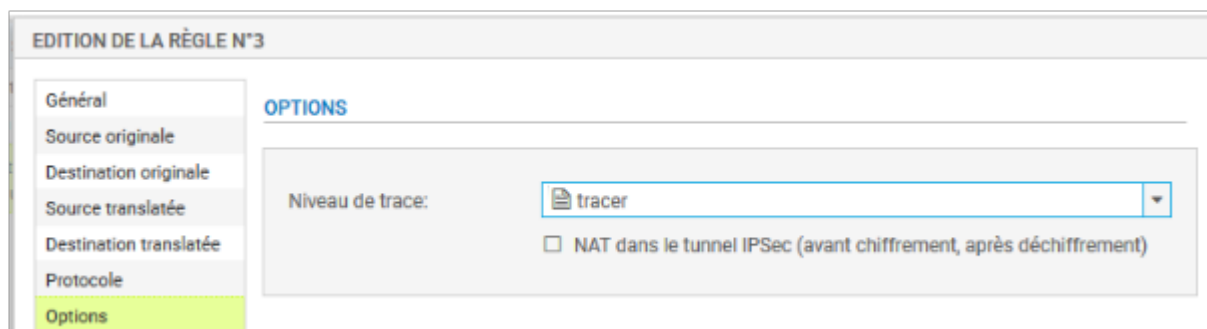
Le détail ci-dessous :



Traçage des règles de NAT

Le traçage des règles de NAT est utilisée à des fins de diagnostic afin de suivre le premier paquet passant dans la règle de NAT concernée.

- Double-cliquer sur la règle que vous voulez tracer et choisissez l'onglet **Options**, et dans niveau de trace **tracer** puis **OK**.



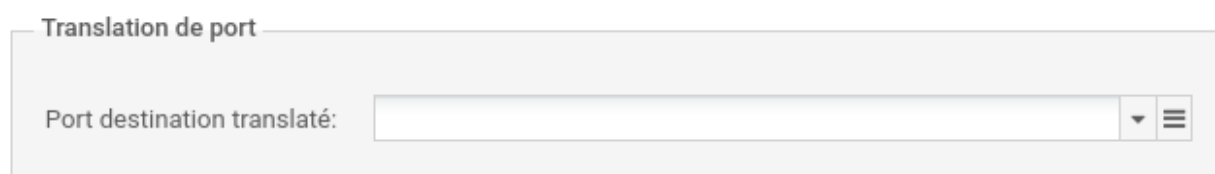
Il est également possible de réaliser une redirection de ports directement lors de la création d'une règle de filtrage (voir fiche 4). L'intérêt d'intégrer le filtrage et la redirection dans une règle unique est d'optimiser les performances puisque le pare-feu réalise un seul traitement au lieu de deux. Voici un exemple ci-dessous équivalent à la règle précédente :



- Dans l'onglet **Destination** de la règle de filtrage, choisissez l'onglet **Configuration avancée**, puis dans **NAT sur la destination**, sélectionner l'objet correspondant à votre serveur web privé :



- Puis dans l'onglet Port/Protocole, choisir any dans la zone Port destination traduité. Si le port après translation est identique au port avant translation, il est recommandé de ne pas le préciser. Laisser vide ou utiliser l'objet any.



Attention, dans ce cas, la règle de NAT n'est pas forcément utilisée. En effet, si une règle qui précède cette dernière (ou une règle implicite) correspond, le paquet n'est plus confronté aux règles suivantes. Alors que ce même paquet est ensuite confronté aux règles NAT.