

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 traduire 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.

ASSISTANT NAT STATIQUE

Objectif : Associer une adresse IP privée et une adresse IP publique (virtuelle).
Par exemple, une correspondance 1 vers 1 entre un serveur local et une IP publique.

Général

ADRESSE IP PRIVÉE

Machine(s) privée(s): srv_ftp_priv

ADRESSE IP VIRTUELLE (PUBLIQUE)

Machine(s) virtuelle(s): srv_ftp_pub

Uniquement sur l'interface: out

Configuration avancée

Uniquement pour les ports: Any

☒ Publication ARP sur la destination externe (publique)

✕ ANNULER
✓ TERMINER

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

- 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.

2	<input checked="" type="checkbox"/>	on	srv_ftp_priv	* Any	interface: out	* Any	→	ARP	srv_ftp_pub
3	<input checked="" type="checkbox"/>	on	* Any	interface: out	ARP	srv_ftp_pub	* Any	→	srv_ftp_priv

• Procédez de manière identique pour le serveur mail : objet **srvmailpriv** et objet **srvmailpub**

4	<input checked="" type="checkbox"/>	on	srv_mail_priv	* Any	interface: out	* Any	→	ARP	srv_mail_pub
5	<input checked="" type="checkbox"/>	on	* Any	interface: out	ARP	srv_mail_pub	* Any	→	srv_mail_priv

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 :

POLITIQUE DE SÉCURITÉ / FILTRAGE ET NAT

(5) AgenceA

Editer

Exporter

FILTRAGE

NAT

Rechercher...

+ Nouvelle règle

✕ Supprimer

↑

↓

Couper

Copier

Coller

Chercher dans les logs

	État	Trafic original (avant translation)			Trafic après translation			
		Source	Destination	Port dest.	Source	Port src.	Destination	Port dest.
1	<div><div></div><div>on</div></div>	Network_internals	Internet interface: out	* Any	Firewall_out	ephemeral_fw	* Any	
2		* Any	interface: out	* Any	ARP		srv_ftp_pub	

Cette règle a été utilisée 856 fois

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 **srvwebpub**, 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 = **FirewallOut**, * **Port dest= http**, * **Source tradatée = Any**, * **Destination tradatée = srvwebpriv**, * **Port destination tradatée = ephemeralfw**.

6	<input checked="" type="checkbox"/>	on	Internet	Firewall_out	http	→	* Any	srv_web_priv	ephemeral
---	-------------------------------------	----	----------	--------------	------	---	-------	--------------	-----------

==== Traçage des règles de NAT =====

Étape 4 : Vous allez activer 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. ===== Retour Accueil Stormshield ===== * [Stormshield](#)

From:

/ - Les cours du BTS SIO

Permanent link:

</doku.php/reseau/stormshield/fiche4?rev=1632084947>

Last update: **2021/09/19 22:55**

