Fiche savoirs : la translation d'adresses

Présentation

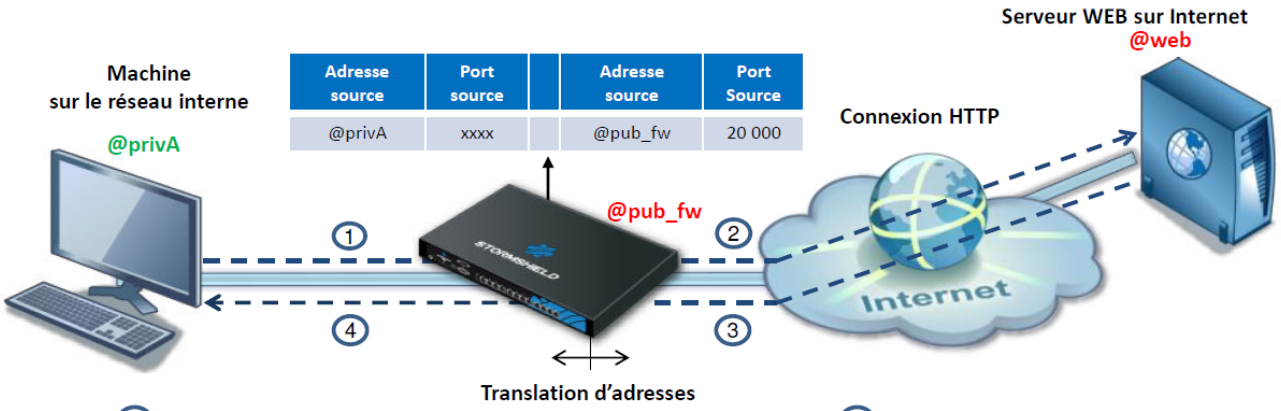
Les **réseaux privés** utilisent des plages d'adresses IP qui ne sont **pas routées sur Internet** (RFC 1918).

Le mécanisme de **NAT** (Network Address Translation) permet de **modifier** les **adresses IP** source/destination et les **ports** source/destination d'un paquet IP pour permettre :

- à des ordinateurs d'un réseau privé d'**accéder à Internet** : il sagit du **NAT dynamique** ou **NAPT** ;
- d'**accéder** depuis internet à des **serveurs d'un réseau privé** : il s'agit du **NAT Statique** :
  - par **redirection de port** ;
  - ou par **association** d'une **adresse IP publique** à une **adresse IP privée**.

Translation dynamique

Objectif : Translater un réseau privé en une (ou plusieurs) adresse IP publique



Paquet original (1)

Adresse Source	Port Source	Adresse Destination	Port Destination
@privA	xxxx	@Web	80

Paquet translaté (2)

Adresse Source	Port Source	Adresse Destination	Port Destination
@pub_fw	20 000	@Web	80

Paquet translaté (4)

Adresse Source	Port Source	Adresse Destination	Port Destination
@Web	80	@privA	xxxx

Paquet original (3)

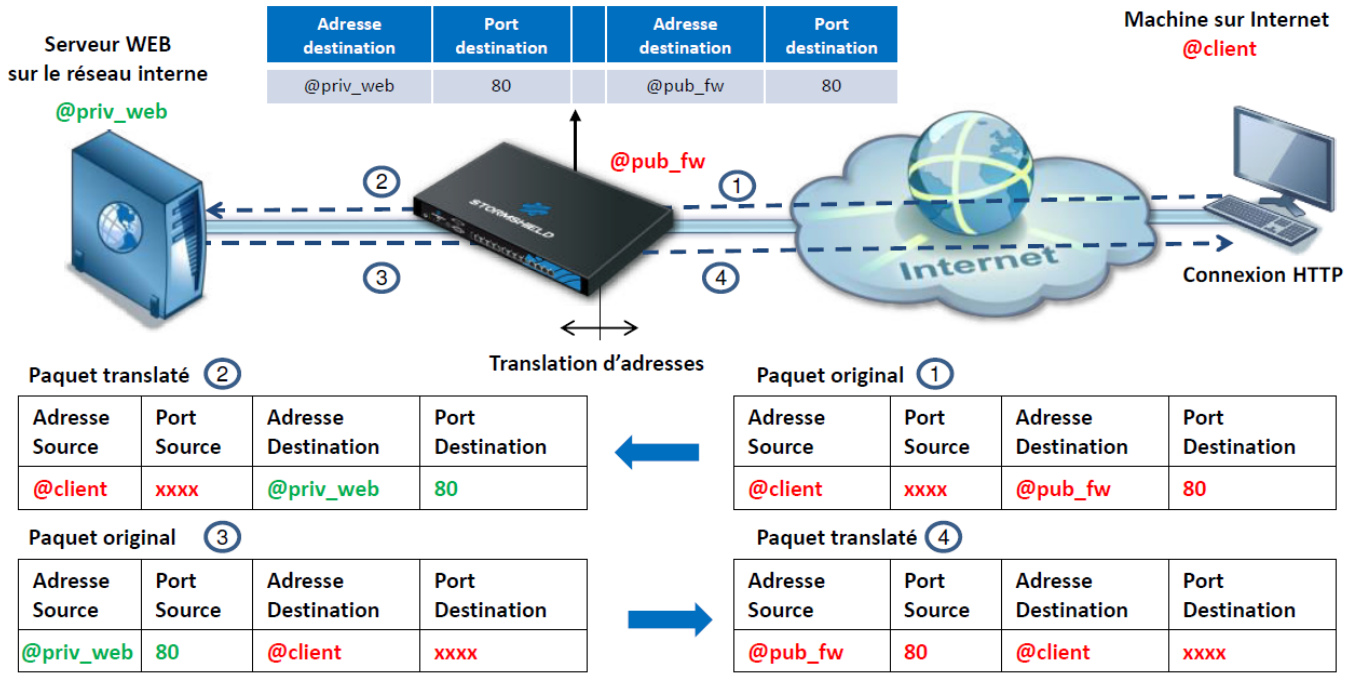
Adresse Source	Port Source	Adresse Destination	Port Destination
@Web	80	@pub_fw	20 000

- le paquet IP prevenant d'un ordinateur du réseau privé est modifié par le pare-feu :
  - l'adresse IP source privée de l'ordinateur est remplacée par l'adresse IP publique du pare-feu
  - le port source de l'ordinateur est remplacé par un port dans la plage [20 000 - 59 9999].

Le pare-feu garde mémoire de la correspondance de translation entre (l'adresse IP « @privA »/port source « xxxx ») et (l'adresse IP « @pub*fw »/port source 20000). Cette correspondance est utilisée pour translater les réponses en provenance du serveur WEB en remplaçant (l'adresse IP destination « @pub*fw »/port destination 2000) par (l'adresse IP destination « @privA »/port destination « xxxx »).

Translation statique par port

Objectif : Donner accès à des serveurs internes du réseau privé depuis Internet avec l'adresse adresse IP publique du pare-feu



Adresse destination	Port destination		Adresse destination	Port destination
@priv_web	80		@pub_fw	80

Adresse Source	Port Source	Adresse Destination	Port Destination
@client	xxxx	@priv_web	80

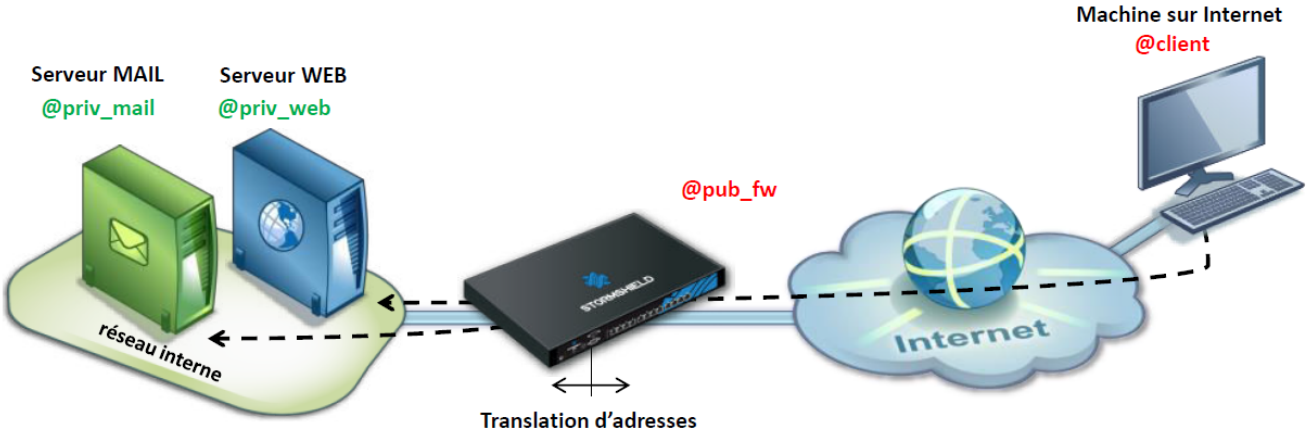
Adresse Source	Port Source	Adresse Destination	Port Destination
@client	xxxx	@pub_fw	80

Adresse Source	Port Source	Adresse Destination	Port Destination
@priv_web	80	@client	xxxx

Adresse Source	Port Source	Adresse Destination	Port Destination
@pub_fw	80	@client	xxxx

La **translation statique par port**, appelé communément **redirection de port**, permet de rendre accessible des services hébergés dans un réseau local via une seule adresse IP publique du pare-feu.

Plusieurs services peuvent ainsi êtree publiés :

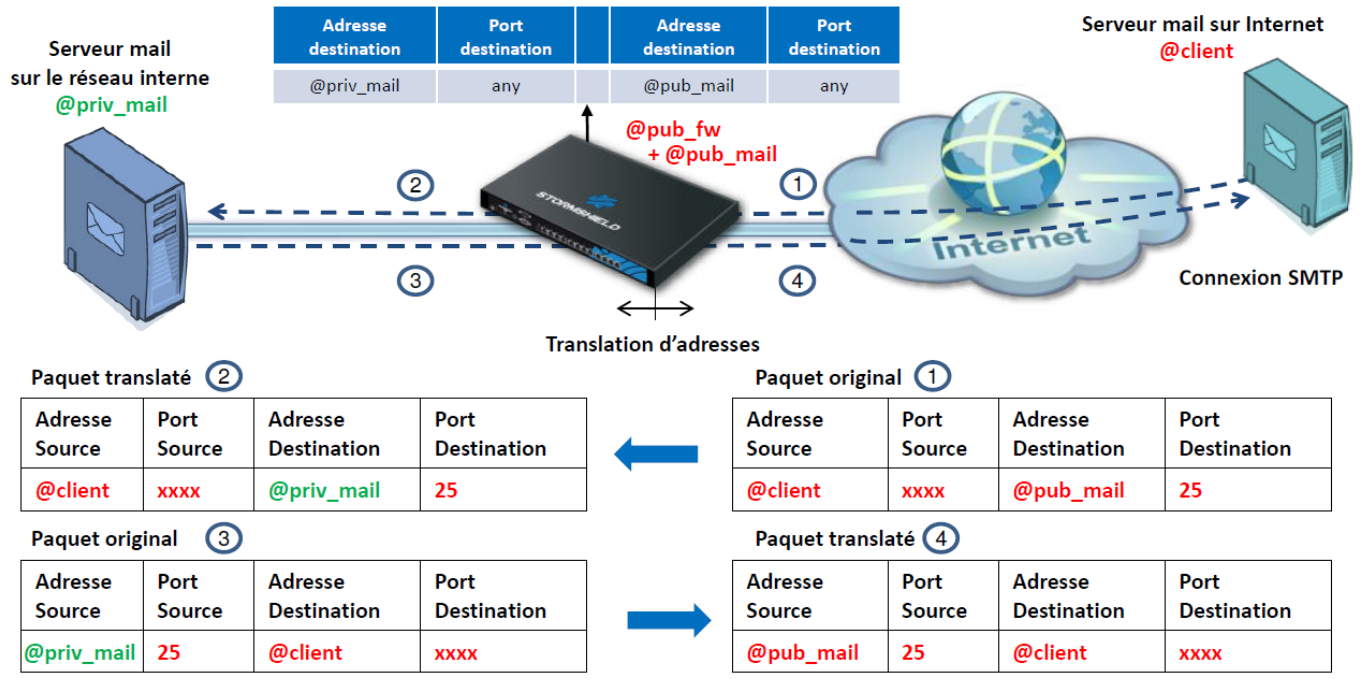


Adresse destination	Port destination		Adresse destination	Port destination
@priv_web	80		@pub_fw	80
@priv_mail	25		@pub_fw	25

Translation statique

Objectif : Dédier une adresse IP publique à un serveur interne du réseau privé.

Connexion entrante



Paquet translaté (2)

Adresse Source	Port Source	Adresse Destination	Port Destination
@client	xxxx	@priv_mail	25

Paquet original (1)

Adresse Source	Port Source	Adresse Destination	Port Destination
@client	xxxx	@pub_mail	25

Paquet original (3)

Adresse Source	Port Source	Adresse Destination	Port Destination
@priv_mail	25	@client	xxxx

Paquet translaté (4)

Adresse Source	Port Source	Adresse Destination	Port Destination
@pub_mail	25	@client	xxxx

Il est nécessaire de disposer d'au moins deux adresses IP publiques poru le pare-feu :

- une adresse IP publique configurée sur l'interface externe du pare-feu
- une adresse IP publique supplémentaire uytilisée dans la règle de translation.

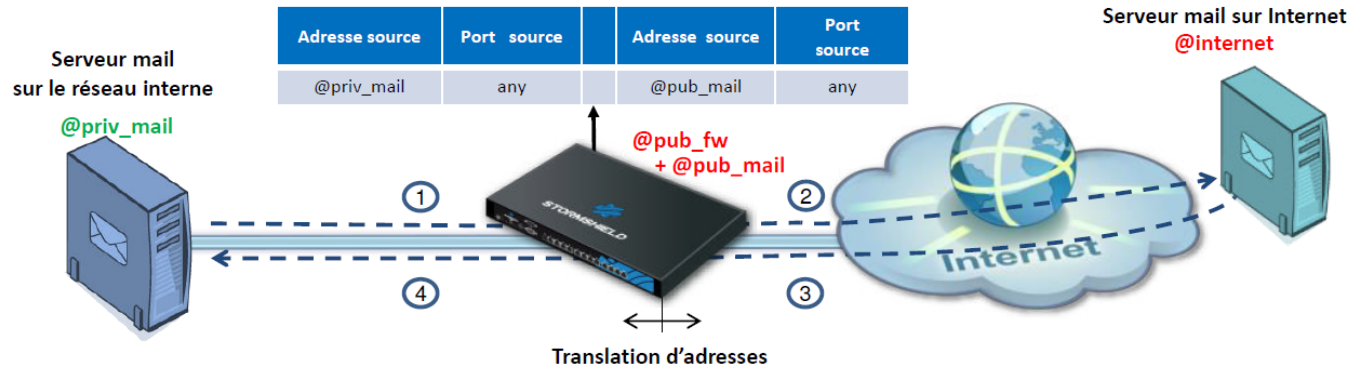
La translation statique doit être bidirectionnelle :

- le serveur local est accessible depuis internet, avec son adresse IP publique
- les connexions sortantes initiées par ce serveur vers internet doivent avoir comme source la même adresse IP publique.

Ceci nécessite deux règles de translation :

- une règle pour les connexions entrantes
- et une autre règle pour les connexions sortantes.

connexion sortante



Paquet original (1)

Adresse Source	Port Source	Adresse Destination	Port Destination
@priv_mail	xxxx	@internet	25

Paquet translaté (2)

Adresse Source	Port Source	Adresse Destination	Port Destination
@pub_mail	xxxx	@internet	25

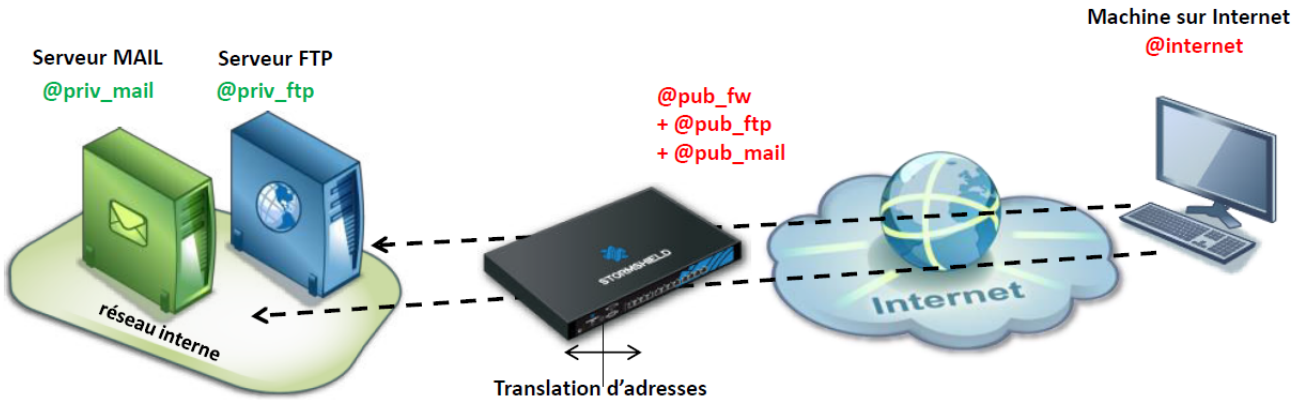
Paquet translaté (4)

Adresse Source	Port Source	Adresse Destination	Port Destination
@internet	25	@priv_mail	xxxx

Paquet original (3)

Adresse Source	Port Source	Adresse Destination	Port Destination
@internet	25	@pub_mail	xxxx

Exemples des règles de translation :



Adresse source	Port source	Adresse destination	Port destination		Adresse source	Port source	Adresse destination	Port destination
@priv_mail	Any	Internet	Any		@pub_mail	any		
Internet	Any	@pub_mail	Any				@priv_mail	
@priv_ftp	Any	Internet	Any		@pub_ftp	Any		
internet	Any	@pub_ftp	Any				@priv_ftp	

- Publication ARP des adresses IP publiques virtuelles Comme les adresses IP publiques virtuelles ne sont pas configurées sur l'interface externe du pare-feu, celui-ci ne répondra pas aux requêtes ARP pour la résolution de ces adresses IP en adresse MAC du pare-feu.

Il est alors nécessaire d'activer la publication ARP des adresses IP publiques virtuelles pour le fonctionnement de la translation statique. Cela ajoute une entrée dans la table ARP du pare-feu pour faire la correspondance entre chaque adresse IP publique virtuelle et l'adresse MAC de l'interface externe.

Création d'une règle NAT statique

L'assistant de création **règle de NAT statique (bimap)** permet de renseigner :

- l'adresse IP **privée** et l'adresse IP **publique virtuelle** du serveur interne,
- l'interface externe du pare-feu depuis laquelle le serveur sera accessible,
- le ou les **ports d'écoute** du serveur
- d'activer la **publication ARP**.

L'assistant ajoute deux règles de translation :

- une règle pour la translation des flux sortants **du serveur interne vers le réseau public, * une deuxième règle pour les flux entrants à destination de l'adresse IP publique virtuelle. Les deux règles peuvent être ensuite modifiées par la suite indépendamment l'une de l'autre. Translation ==== Retour ==== * Mise en oeuvre de l'UTM Stormshield**