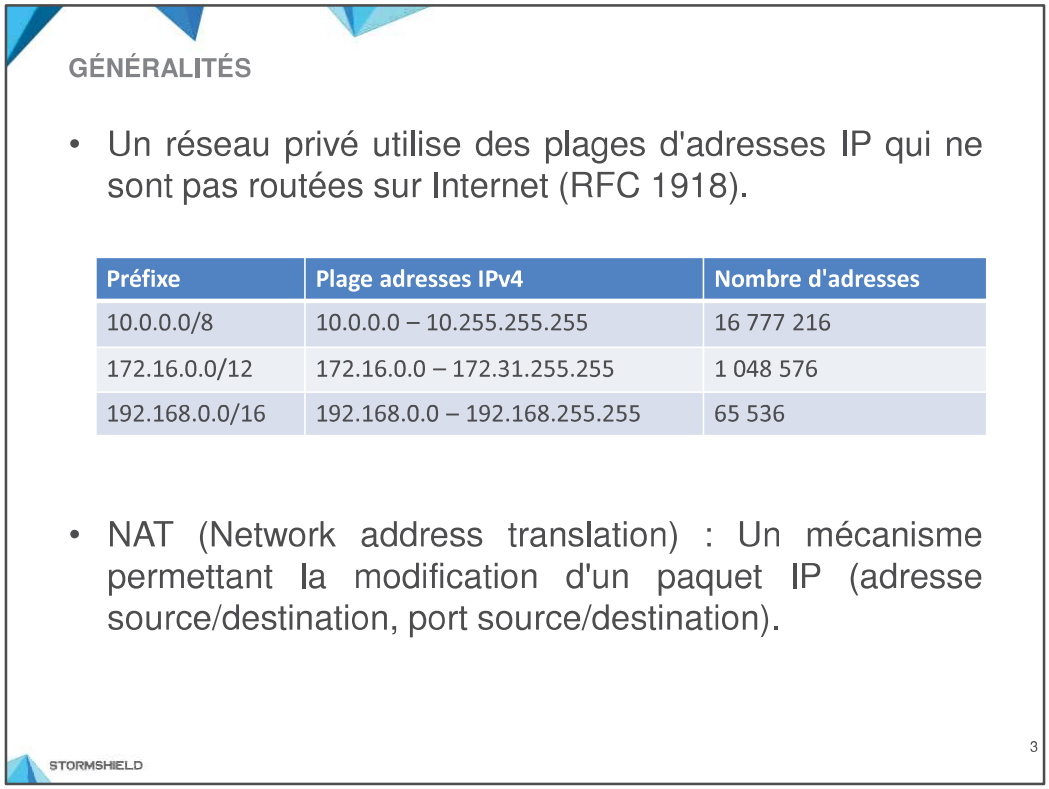
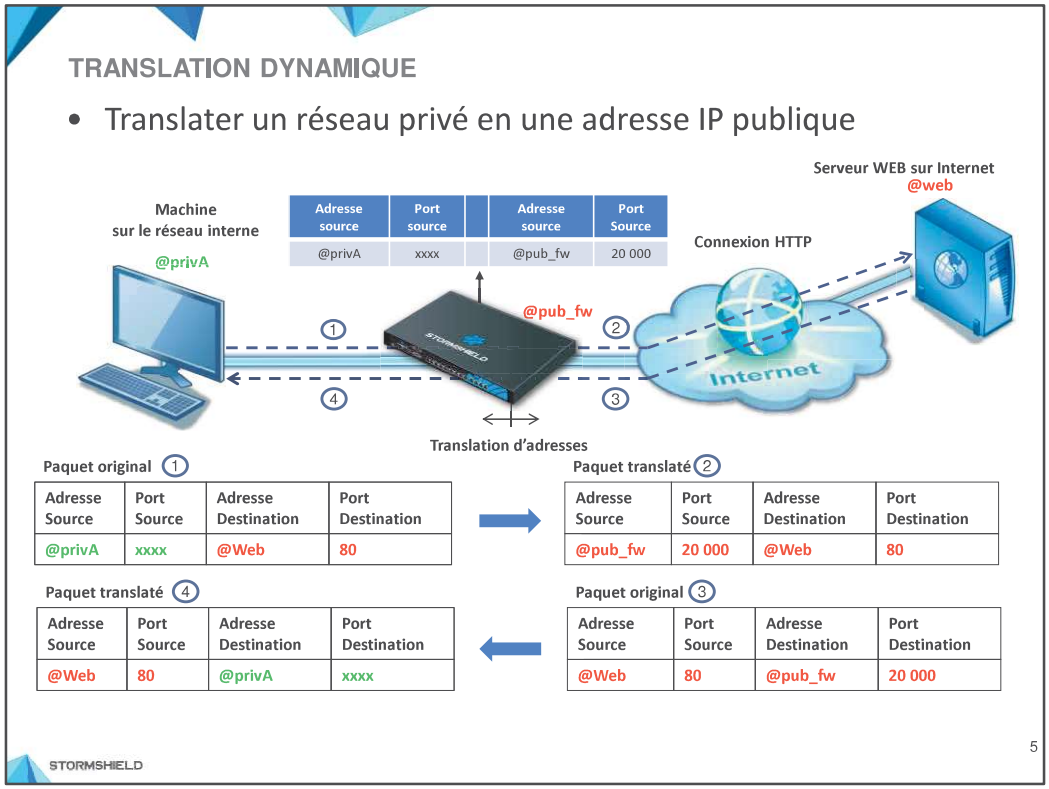
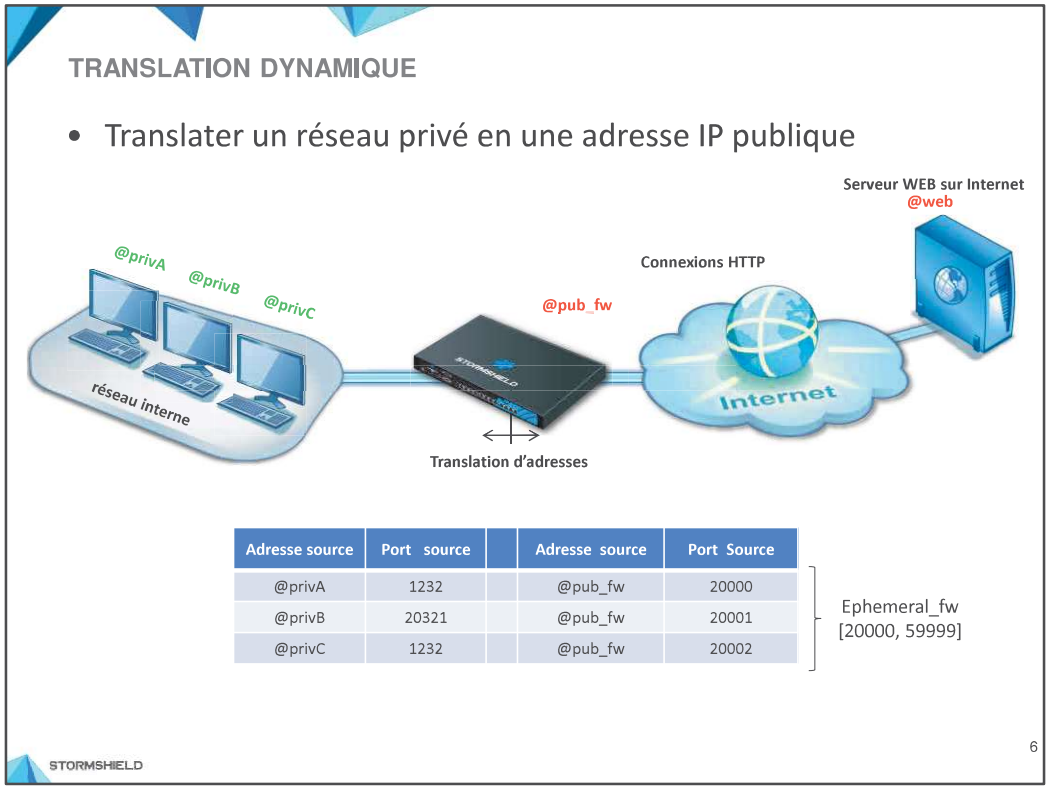


Les mécanismes de translation d'adresses ont été mis au point pour faire face à la pénurie d'adresses IP publiques. Le principe de base consiste à utiliser des adresses IP privées, définies par l'IANA (Internet Assigned Numbers Authority) et renseignées par la RFC 1918 (tableau ci-dessus), pour les réseaux locaux des entreprises et des particuliers, et de relier ces réseaux à Internet via une seule adresse IP publique.



Dans la majorité des cas, ce type de translation est mis en œuvre pour permettre à un réseau local configuré avec des adresses IP privées d'accéder à Internet via une seule adresse IP publique.

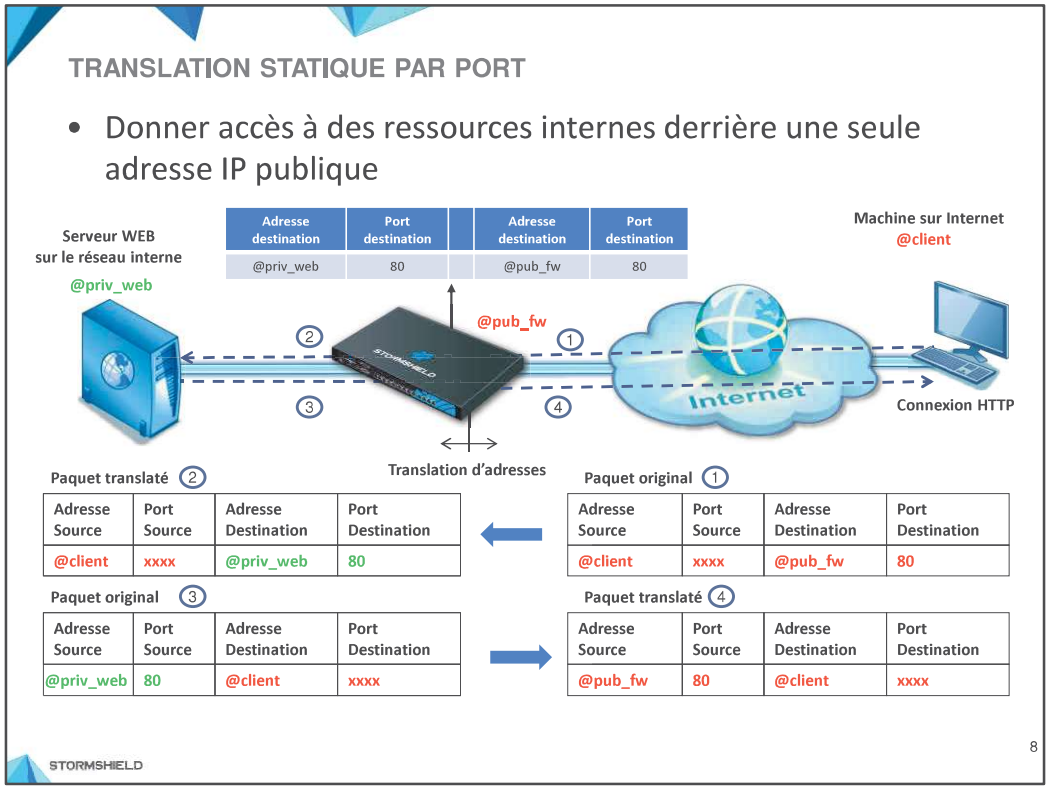
La figure ci-dessus illustre le fonctionnement de ce type de translation lorsque la machine « @privA » accède à un serveur WEB « @web » sur internet. Le paquet IP transmis par la machine « @privA » vers le serveur « @web » est intercepté par le firewall qui remplace l'adresse IP source « @privA » par l'adresse IP publique du firewall « @pub_fw » et le port source « xxxx » (ce port est choisi par le système d'exploitation de la machine « @privA ») par un port dans la plage [20000-59999]. Le firewall garde dans sa mémoire 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 »).



La modification du port source se justifie principalement dans le cas où deux machines « @privA » et « @privC » utilisent le même port source pour ouvrir une connexion vers le même serveur WEB. Si le port source n'est pas modifié par le firewall, le serveur web recevra deux demandes de connexion arrivant de la même adresse IP publique « @pub_fw » et même port source ce qui peut engendrer un dysfonctionnement des deux connexions et une ambiguïté de translation des réponses au niveau du firewall. Ce dernier ne pourra pas savoir à quelle machine il faudra renvoyer les réponses reçues du serveur.

Les ports sources fixés par le firewall sont choisis dans une plage prédéfinie appelée ephemeral_fw [20000-59999]. Par défaut, les ports sont choisis séquentiellement dans la plage, cependant une option est disponible pour permettre un choix aléatoire.

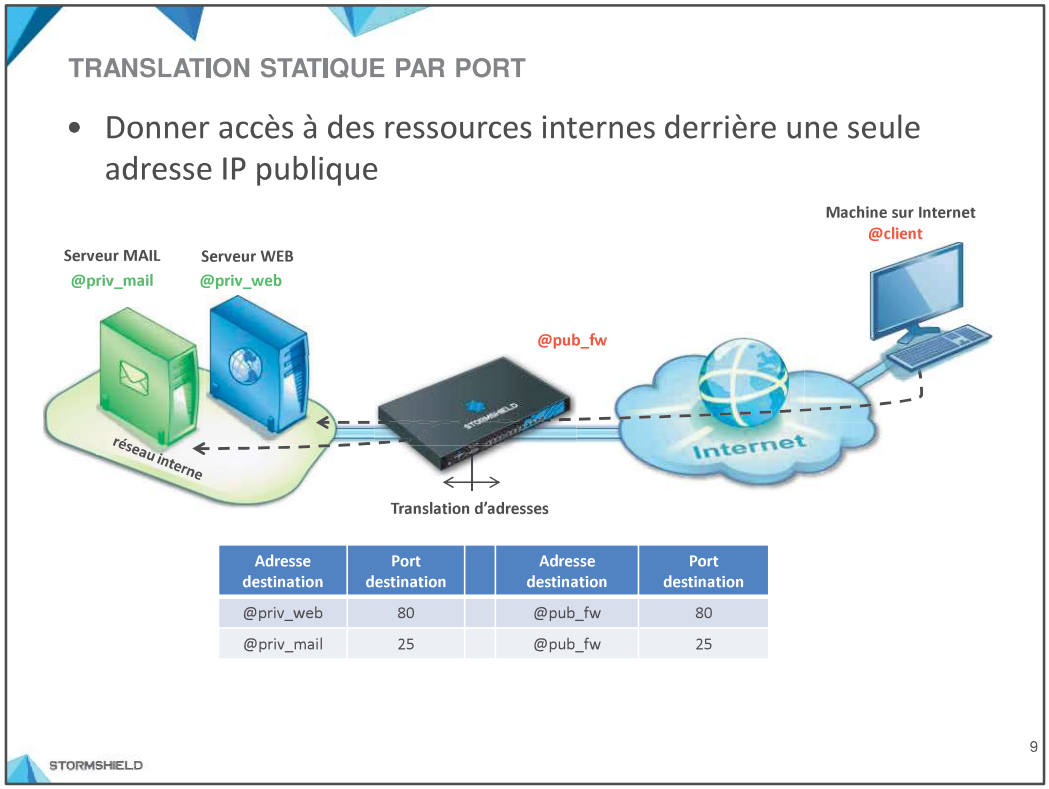
Il est possible d'utiliser une plage d'adresses pour masquer l'adresse IP source.
La règle de NAT utilisera un objet de type réseau ou plage d'adresses à la place d'un objet de type hôte dans le champ *Source* de *Trafic après translation*. La translation se faisant avec une correspondance 1:1 entre les plages, elles doivent être de la même taille. Il est alors obligatoire de ne pas translater le port source.



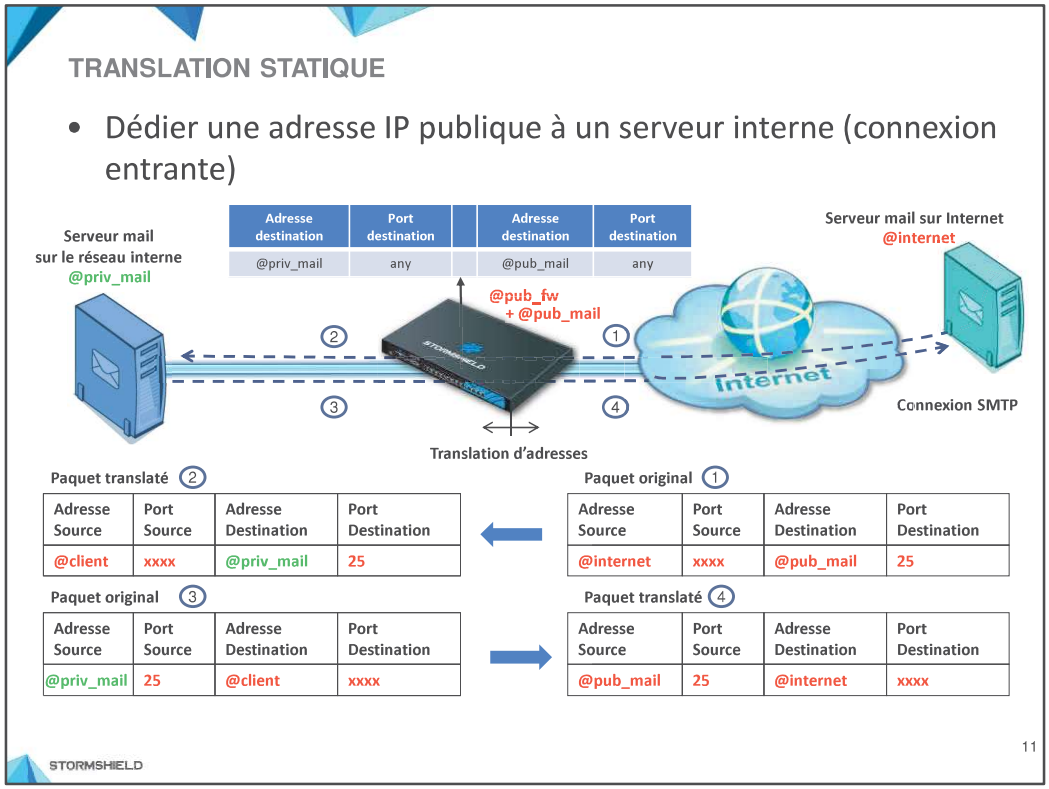
Ce type de translation, appelé communément « redirection de port », permet de rendre accessible des services hébergés dans un réseau local via une seule adresse IP publique.

La figure ci-dessus illustre l'exemple d'un serveur web local « @priv_web » accessible depuis internet sur l'adresse IP publique du firewall « @pub_fw ». Au niveau du firewall, une règle de translation est créée pour la correspondance entre (l'adresse IP publique destination « @pub_fw »/port destination 80) et (l'adresse IP du serveur local « @priv_web »/port destination 80).

Ainsi, le paquet émis par la machine « @client » vers l'adresse IP « @pub_fw » sur le port 80 est modifié pour être renvoyé vers le serveur web sur le même port. Et la réponse renvoyée par ce serveur est également modifiée en conséquence avant d'être renvoyée vers la machine « @client ». Il est important de noter que les ports destination avant et après translation peuvent être différents.



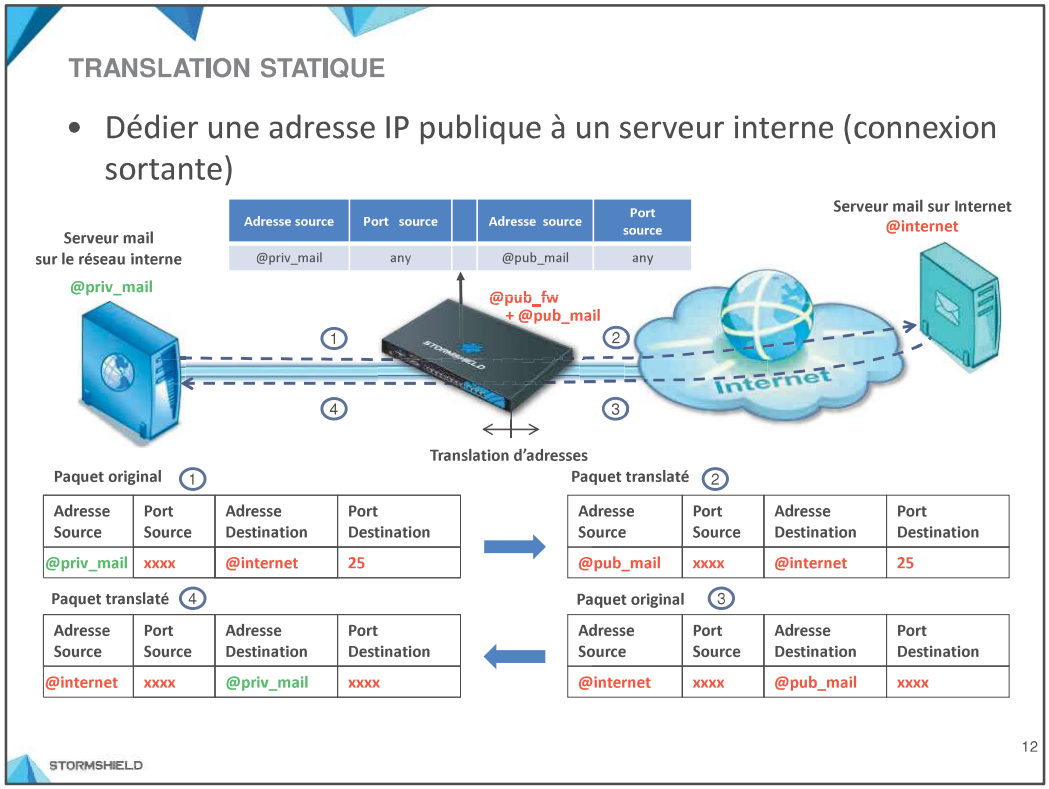
Il est possible de rendre accessibles plusieurs services hébergés sur plusieurs serveurs locaux via une seule adresse IP publique comme l'illustre la figure ci-dessus. La distinction entre les serveurs se base uniquement sur le numéro de port du service.



Ce type de translation permet de dédier une adresse IP publique à un serveur local configuré avec une adresse IP privée. Ceci suppose qu'on dispose d'au moins deux adresses IP publiques : « @pub_fw » configurée sur l'interface externe du firewall et « @pub_mail » employée au niveau des règles de translation.

La translation statique doit être bidirectionnelle, ce qui signifie que le serveur local est accessible pour les connexions entrantes, depuis Internet, avec son adresse IP publique et les connexions sortantes initiées par ce serveur vers internet doivent avoir comme source la même adresse IP publique. Ceci se traduit par deux règles de translation : une règle pour les connexions entrantes et une autre règle pour les connexions sortantes.

La figure ci-dessus, illustre les modifications que subissent les paquets d'une connexion entrante vers un serveur mail local en se basant sur la règle de translation qui fait la correspondance entre (l'adresse IP publique destination « @pub_mail ») et (l'adresse IP du serveur local « @priv_mail »).
Ainsi, le paquet émis par le serveur mail « @internet » vers l'adresse IP « @pub_mail » est modifié pour être renvoyé vers le serveur mail. Et la réponse renvoyée par ce serveur est également modifiée en conséquence avant d'être renvoyée vers le serveur mail « @internet ». Il est important de noter que les ports source avant et après translation peuvent être restreints à un numéro de port particulier et ils peuvent être différents.

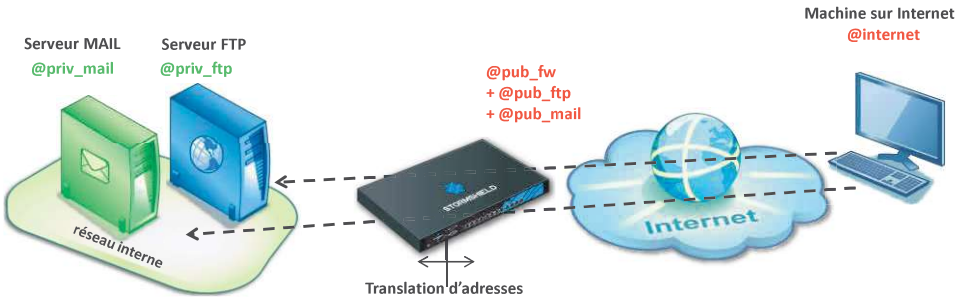


La figure ci-dessus, illustre les modifications que subissent les paquets d'une connexion sortante initiée par le serveur web local vers un serveur sur internet en se basant sur la règle de translation qui fait la correspondance entre (l'adresse IP privée source « @priv_mail ») et (l'adresse IP source publique « @pub_mail »).

Ainsi, le paquet émis par le serveur « @priv_mail » vers une adresse IP sur internet est modifié pour remplacer l'adresse source « @priv_mail » par l'adresse source « @pub_mail ». La réponse renvoyée par le serveur externe est aussi modifiée en conséquence avant d'être renvoyée vers le serveur mail local. Il est important de noter que les ports source avant et après translation peuvent être restreints à un numéro de port particulier et ils peuvent être différents.

TRANSLATION STATIQUE

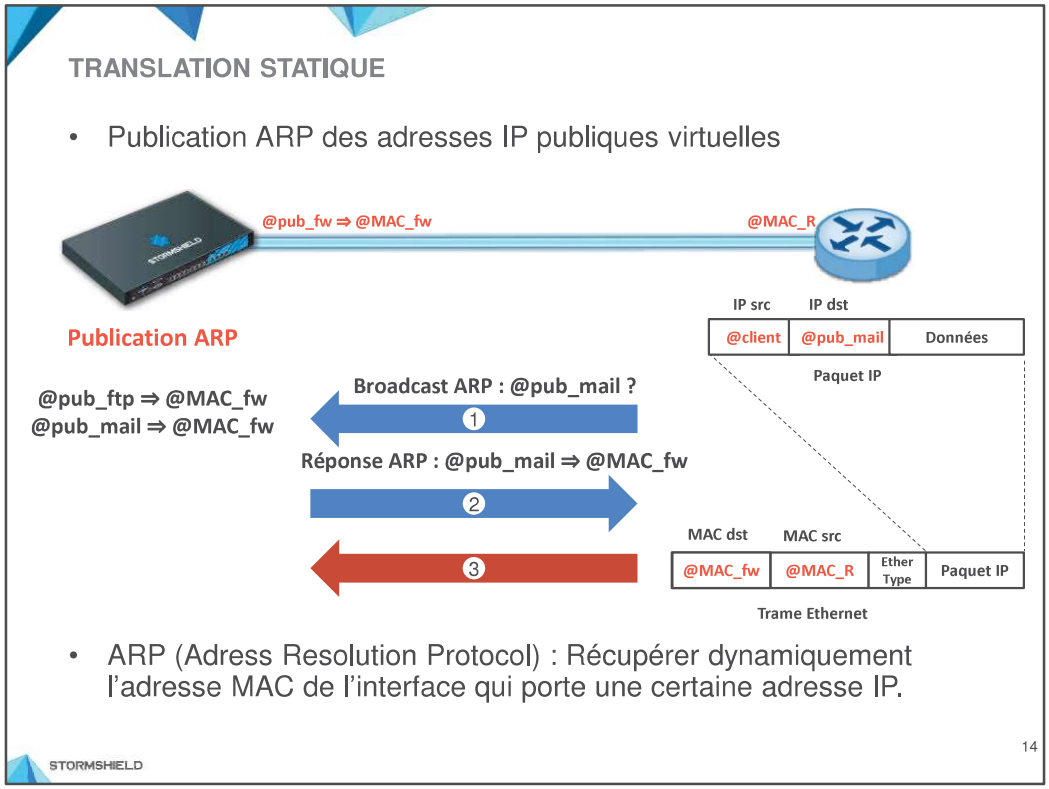
- Dédier une adresse IP publique à un serveur interne



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	

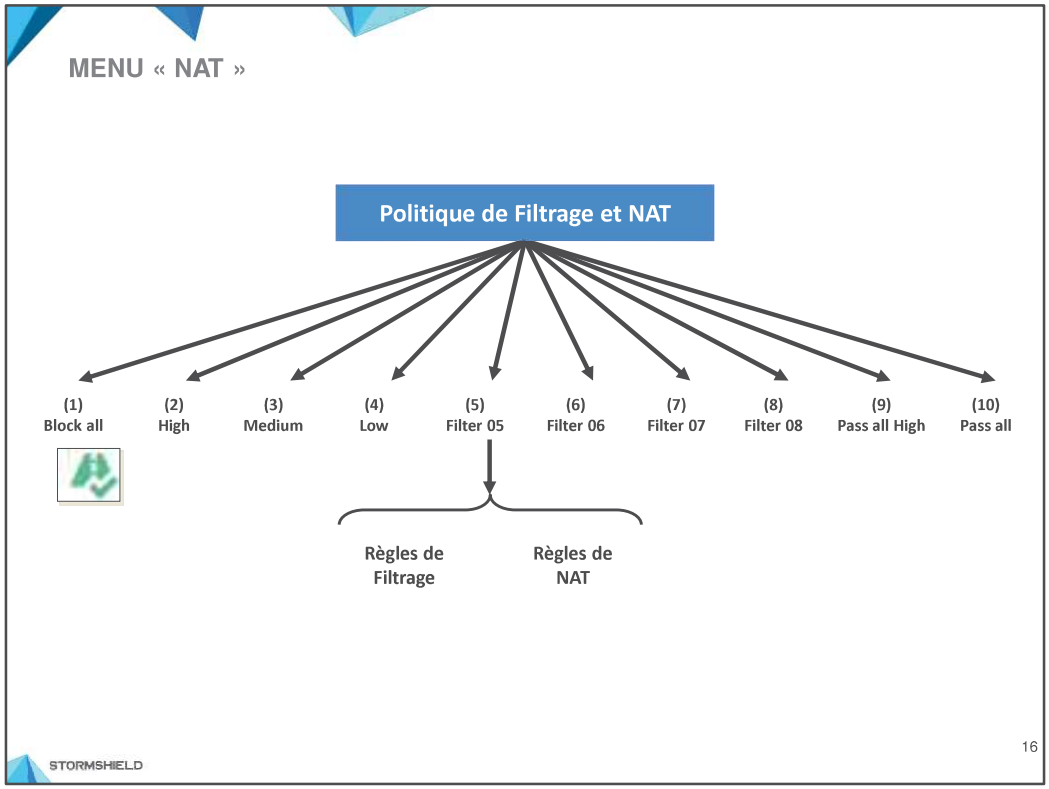
13

Si on dispose de plusieurs adresses IP publiques, il est possible de dédier pour chaque serveur une adresse IP spécifique. Chaque serveur nécessite deux règles de translation présentées ci-dessus.

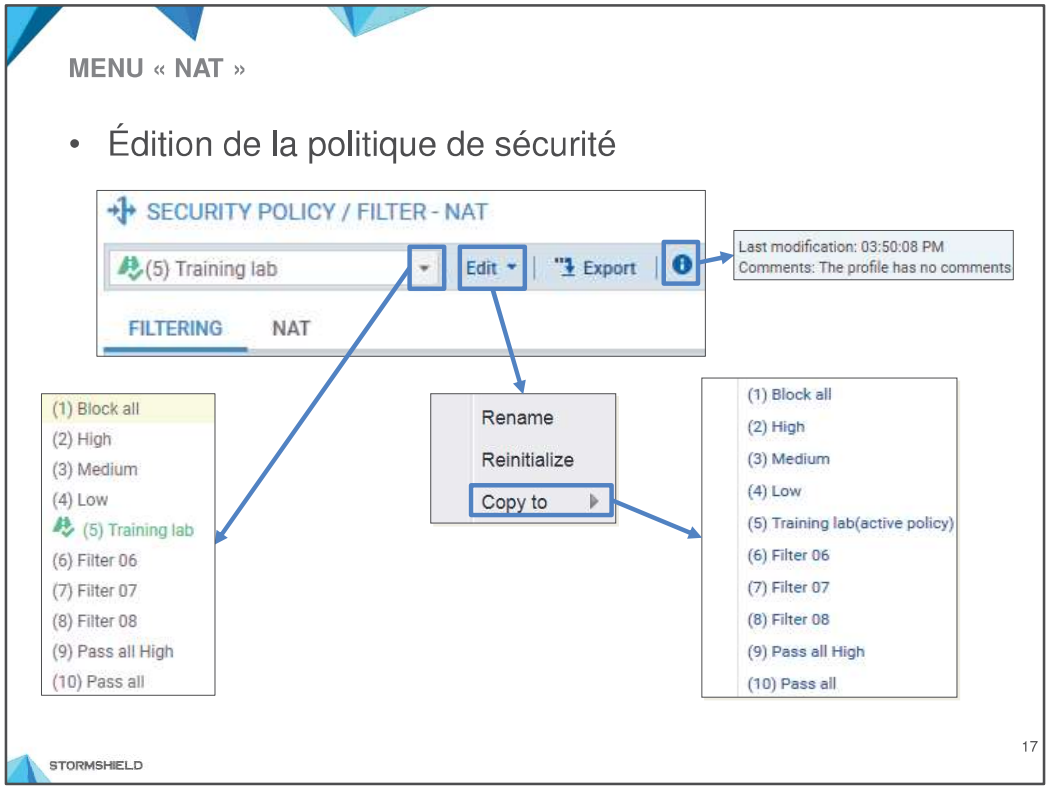


Étant donné que les adresses IP publiques virtuelles ne sont pas configurées sur l'interface externe du firewall, ce dernier ne répondra pas aux requêtes ARP pour la résolution de ces adresses IP en adresse MAC du firewall.

Afin de résoudre ce problème, la publication ARP des adresses IP publiques virtuelles est nécessaire pour le fonctionnement de la translation statique. Elle permet d'ajouter une entrée dans la table ARP du firewall pour faire la correspondance entre chaque adresse IP publique virtuelle et l'adresse MAC de l'interface externe. Ce qui permet au firewall de répondre aux requêtes ARP pour la résolution de ces adresses IP et de recevoir ainsi tous les paquets à leur destination comme l'illustre la figure ci-dessus.



Dans les firewalls Stormshield Network, les règles de filtrage et NAT (translation 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 : 

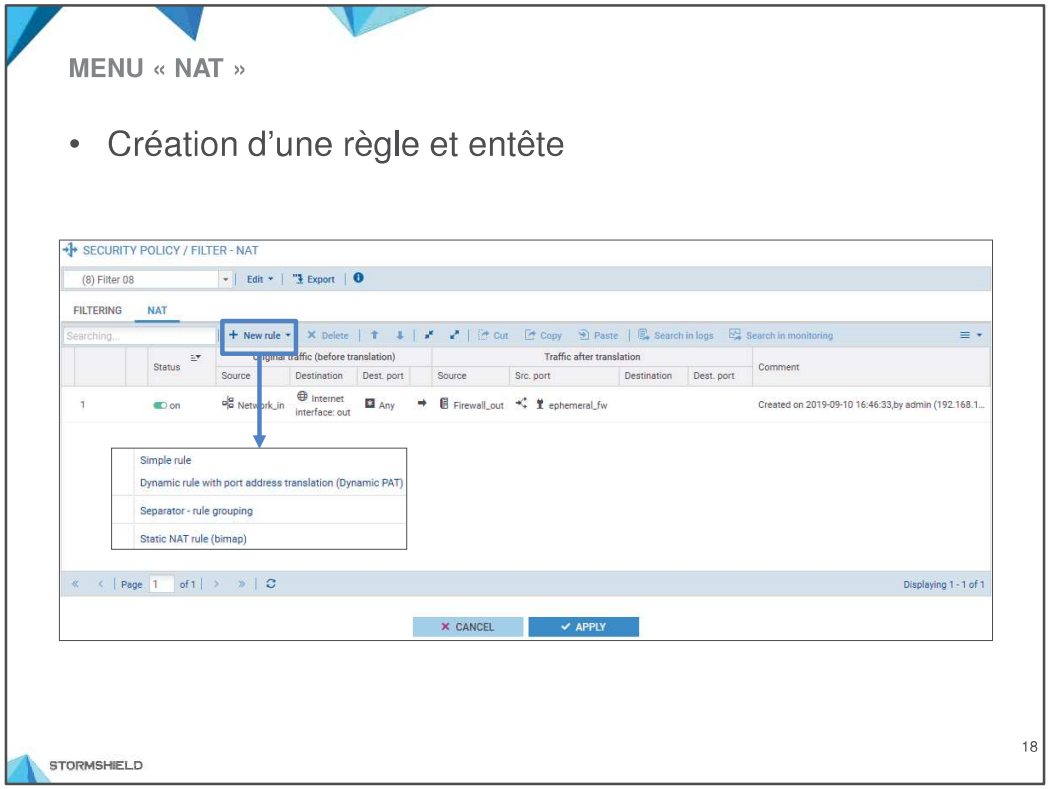


La configuration des règles de filtrage et NAT s'effectue dans le menu **CONFIGURATION ⇒ POLITIQUE DE SÉCURITÉ ⇒ Filtrage et NAT**.
L'entête du menu permet :

- La sélection de la politique de filtrage et NAT grâce à une liste déroulante.
- **Éditer** :
  - **Renommer** : Modifier le nom de la politique.
  - **Réinitialiser** : Remettre les règles de filtrage et NAT par défaut.
  - **Copier vers** : Copier une politique vers une autre.
- **Exporter** : Permet d'exporter les règles de filtrage/NAT de la politique sélectionnée dans un fichier CSV, cet export est utilisé pour récupérer les règles sur un serveur Stormshield Management Center (SMC).

Le reste du menu est composé de deux onglets :

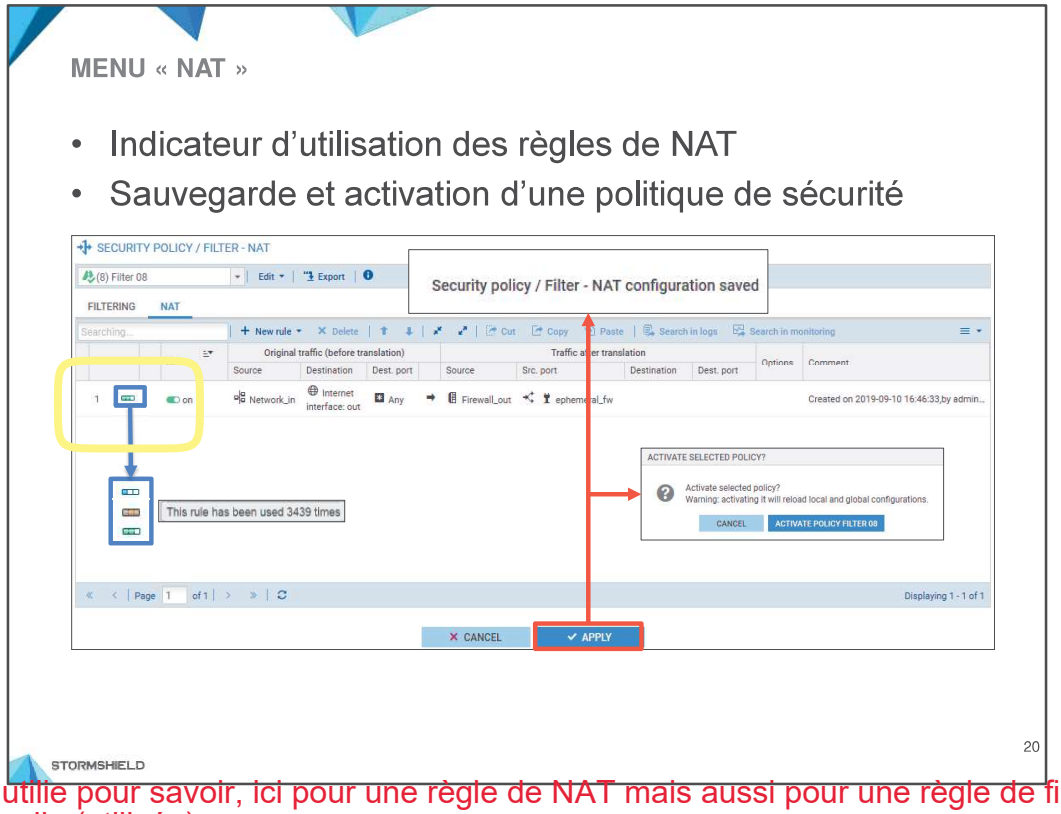
- **Filtrage** : Pour la configuration des règles de filtrage.
- **NAT** : Pour la configuration des règles de translation d'adresses.



L'onglet **NAT** est composé d'un entête pour la gestion des règles de translation:

- **Nouvelle règle** :
  - **Règle standard** : Ajouter une règle de translation standard.
  - **Règle de partage d'adresse source (masquerading)** : Ajouter une règle pour la translation dynamique en précisant la plage de port **ephemeral_fw**.
  - **Séparateur – regroupement de règles** : Ajouter un séparateur de règles qui regroupe toutes les règles se trouvant au dessous, ce qui permet de fermer le séparateur pour masquer l'affichage de toutes les règles lui appartenant. De plus, le séparateur peut être personnalisé par une couleur et un commentaire.
  - **Règle de NAT statique (bimap)** : Lancer un assistant qui facilite l'ajout de règles de translation statique bimap.
- **Supprimer** : Supprimer la/les règle(s) sélectionnée(s).
- **Monter** / **Descendre** : Monter ou descendre la/les règle(s) sélectionnée(s) d'une position dans la liste.
- **Tout dérouler** / **Tout fermer** : Dérouler/fermer tous les séparateurs pour afficher/cacher les règles de NAT.
- **Couper** : Couper la/les règle(s) sélectionnée(s).
- **Copier** : Copier la/les règle(s) sélectionnée(s).
- **Coller** : Coller la/les règle(s) auparavant copiée(s)/coupée(s) de la même ou d'une autre politique.
- **Chercher dans les logs** : Chercher le nom de cette règle dans les journaux d'audit.
- **Chercher dans la supervision** : Chercher le nom de cette règle dans la supervision des connexions.
- **Réinitialiser les statistiques des règles** : Réinitialiser les compteurs de toutes les règles filtrage et NAT de la politique. En positionnant la souris sur l'icône, la date de la dernière réinitialisation s'affiche.
- **Reinit Colonnes** : Réinitialiser l'affichage des colonnes qui compose la fenêtre des règles.

- **Trafic avant translation** : Permet de renseigner les valeurs des paramètres du trafic original.
  - **Source** : L'adresse IP ou le réseau source.
  - **Destination** : L'adresse IP ou le réseau source.
  - **Port dest** : Port destination.
- **Commentaire** : Permet d'ajouter un commentaire. La date, l'heure, l'administrateur et l'adresse IP du PC d'administration sont ajoutés par défaut lors de la création de la règle.
- **Trafic après translation** : Permet de renseigner les nouvelles valeurs des paramètres après translation. Dans le cas où cette partie n'est pas renseignée, le trafic gardera les valeurs originales.
  - **Source** : L'adresse IP ou le réseau source.
  - **Port src** : Port source.
  - **Destination** : L'adresse IP ou le réseau source.
  - **Port dest** : Port destination.
- **Options** : Le passage d'un flux par une règle de translation n'est pas journalisé en mode standard. En mode « Tracer », le trafic est journalisé dans le journal « Filtrage ». La seconde option permet aussi d'activer le NAT dans un tunnel VPN IPSec.
- **Commentaire** : Permet d'ajouter un commentaire. La date, l'heure, l'administrateur et l'adresse IP du PC d'administration sont ajoutés par défaut lors de la création de la règle.

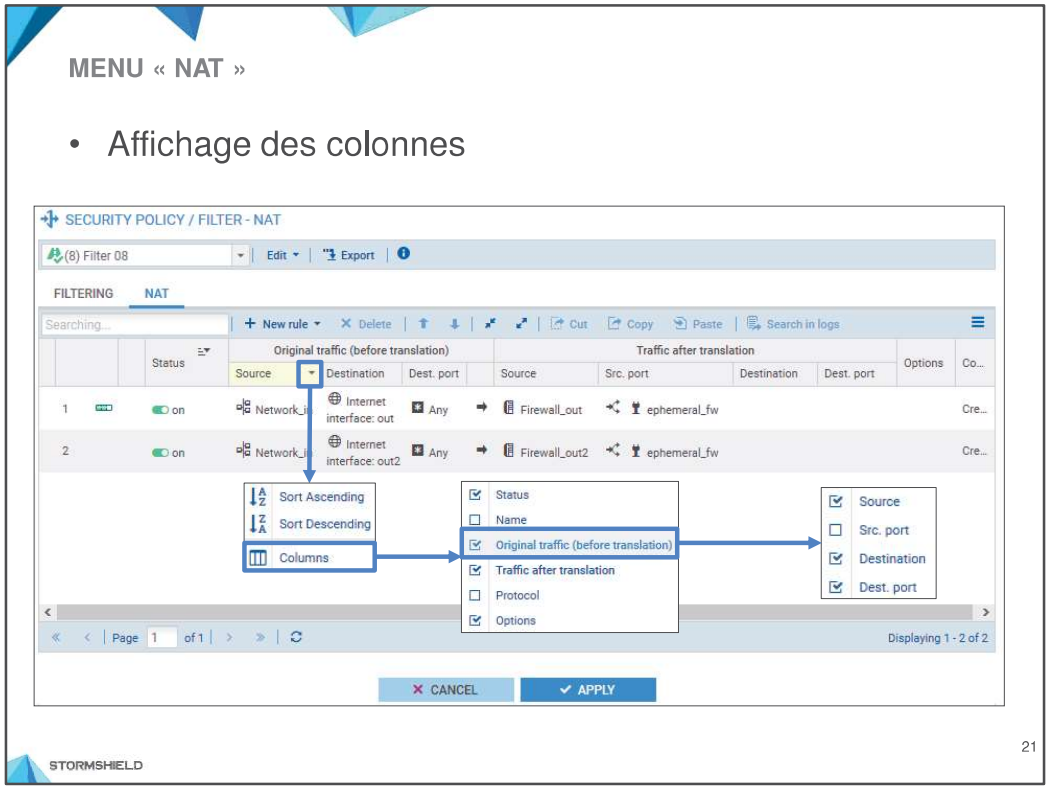


Cela est très utile pour savoir, ici pour une règle de NAT mais aussi pour une règle de filtrage est opérationnelle (utilisée).

L'indicateur d'utilisation (encadré en bleu) précise le nombre de fois où un flux traité correspond aux critères de la règle de traslation. Le compteur numérique s'affiche en passant la souris par dessus. Il peut afficher 4 couleurs qui sont le résultat d'un rapport mathématique entre le nombre de hits de la règle et le nombre de hits maximum atteint par une règle dans le même slot:

- Blanc (vide) : la règle n'a jamais été appliquée,
- Bleue : la valeur affichée est comprise entre 0 et 2% du hit maximal,
- Vert : la valeur affichée est comprise entre 2% et 20% du hit maximal,
- Orange : la valeur affichée est supérieure ou égale à 20% du hit maximal et est supérieure à 10 000 hits.

Pour sauvegarder une politique, il suffit de cliquer sur le bouton **APPLIQUER**. La sauvegarde est immédiate, une nouvelle fenêtre s'ouvre, permettant par ailleurs de rendre la politique active, ou pas, en cliquant sur le bouton **OUI, ACTIVER LA POLITIQUE**, ou **PLUS TARD**.



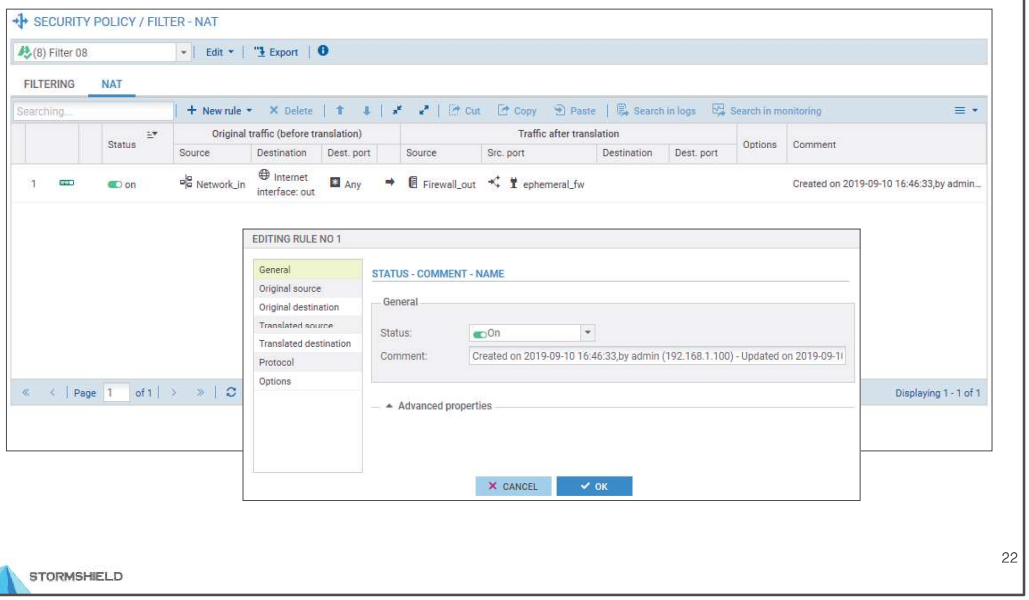
L'affichage des colonnes de la fenêtre peut être personnalisé en cliquant sur l'icône indiquée par la flèche bleue ci-dessus, ensuite sur colonnes. Il suffit de sélectionner une colonne pour qu'elle s'affiche.
Les règles de NAT peuvent être déplacées dans la fenêtre par un glisser/déposer en cliquant à gauche sur le numéro de la règle.

NOTE : La recherche dans les logs ou la supervision s'effectuant sur le nom d'une règle, vous pouvez afficher la colonne **Nom**, remarquez alors qu'une règle a forcément un nom par défaut, modifiable par l'administrateur.

MENU « NAT »

- Paramètres d'une règle

Vous mettrez cela en oeuvre dans les activités
-> à voir pour connaître la démarche à suivre

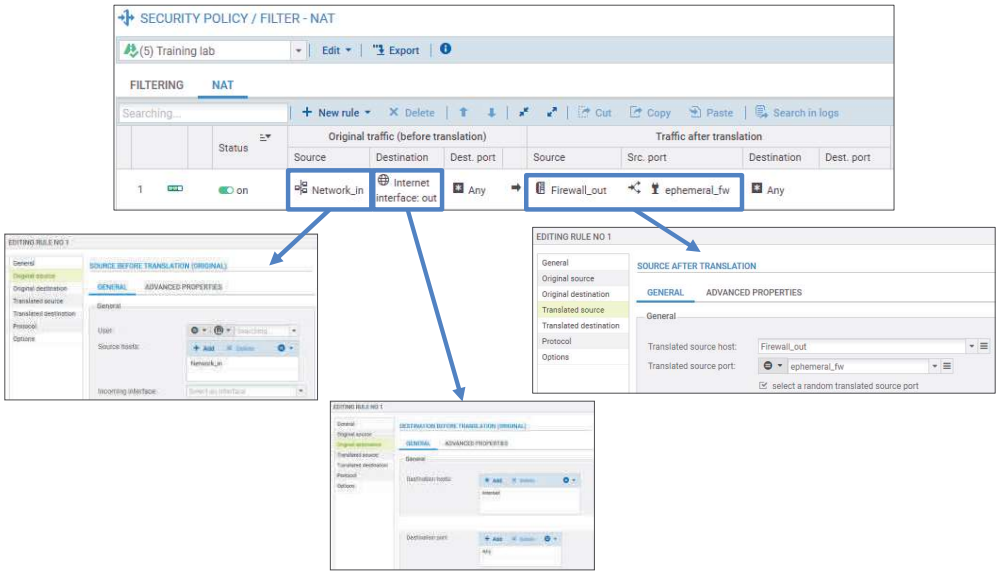


Les paramètres d'une règle peuvent être renseignés directement dans la fenêtre des règles ou sur une nouvelle fenêtre qui s'affiche en double cliquant sur n'importe quel paramètre de cette règle. Cette fenêtre permet aussi l'accès aux paramètres de configuration avancée.
Les valeurs des paramètres étant des objets, ils peuvent être copiés d'une règle à une autre par un simple glisser/déposer.

MENU « NAT »

Vous mettrez cela en oeuvre dans les activités
-> à voir pour connaître la démarche à suivre

- Translation dynamique



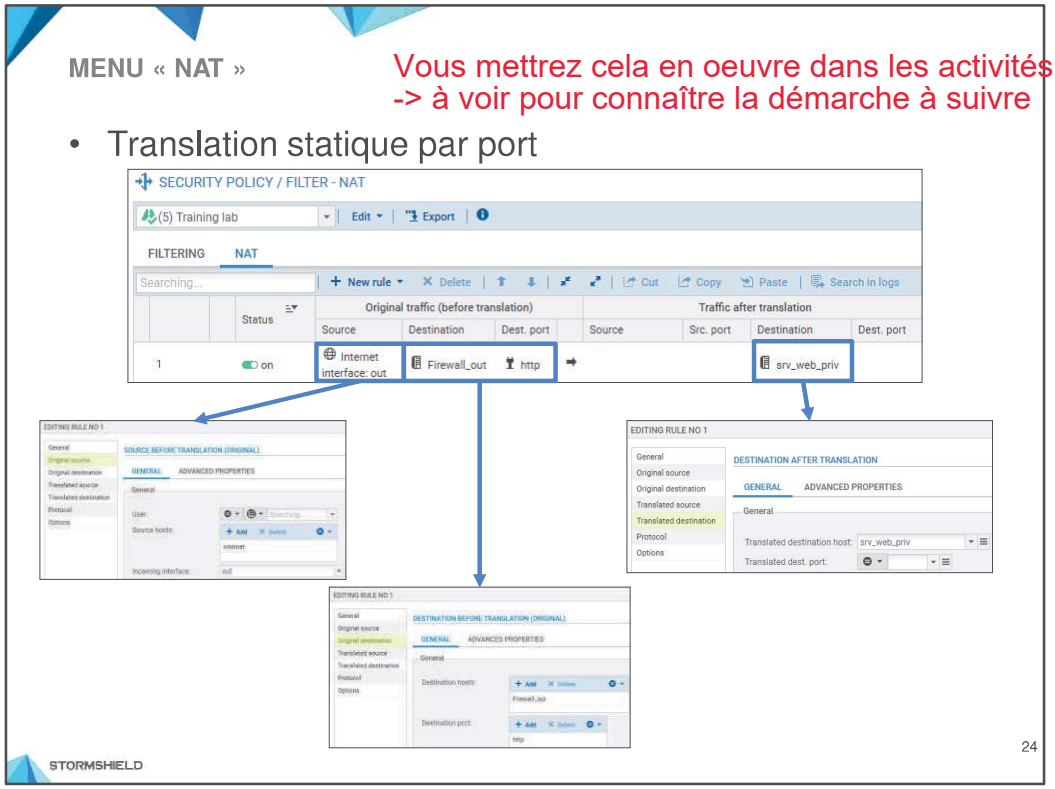
STORMSHIELD

23

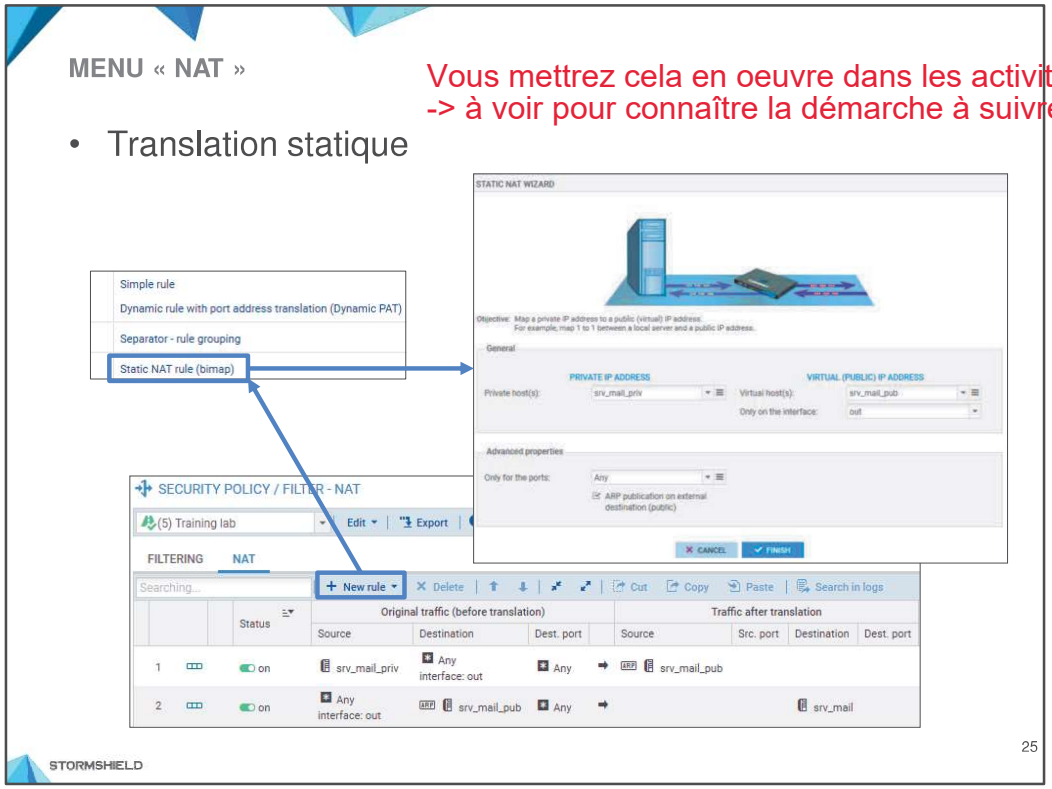
La règle de NAT dynamique est créée avec le bouton **Nouvelle règle ⇒ règle de partage d'adresse source (masquerading)** qui ajoute automatiquement la plage de ports **ephemeral_fw** au niveau du **port src** dans le trafic après translation.

La figure ci-dessus présente un exemple d'une règle de NAT dynamique avec les principaux paramètres qui doivent être renseignés. Dans la section **Trafic original (avant translation)**, la source représente le réseau interne **Network_in** accessible depuis l'interface « in » qui veut accéder à n'importe quelle destination sur n'importe quel port destination. Dans la section **Trafic après translation**, la source est modifiée par l'adresse IP publique portée par l'interface « out » et le port source est translaté part un numéro de port dans la plage **ephemeral_fw**.

Il est conseillé de cocher l'option **choisir aléatoirement le port source translaté** qui permet de choisir aléatoirement un numéro de port dans la plage **ephemeral_fw** pour les nouvelles connexions. Cette option offre une protection contre certaines attaques en rendant le port translaté moins prédictible.



La règle de NAT statique par port est créée à partir d'une **règle standard**. Un exemple est présenté dans la figure ci-dessus.
Dans la section Trafic original, la source représente n'importe quelle machine sur le réseau public, ayant pour destination l'adresse IP publique du firewall sur le port 80 (HTTP). Dans la section trafic après translation, l'adresse IP destination est remplacée par l'adresse IP privée du serveur et le numéro de port 80 (HTTP) est maintenu comme port destination. Il est important de noter que les ports destination avant et après translation peuvent être différents.

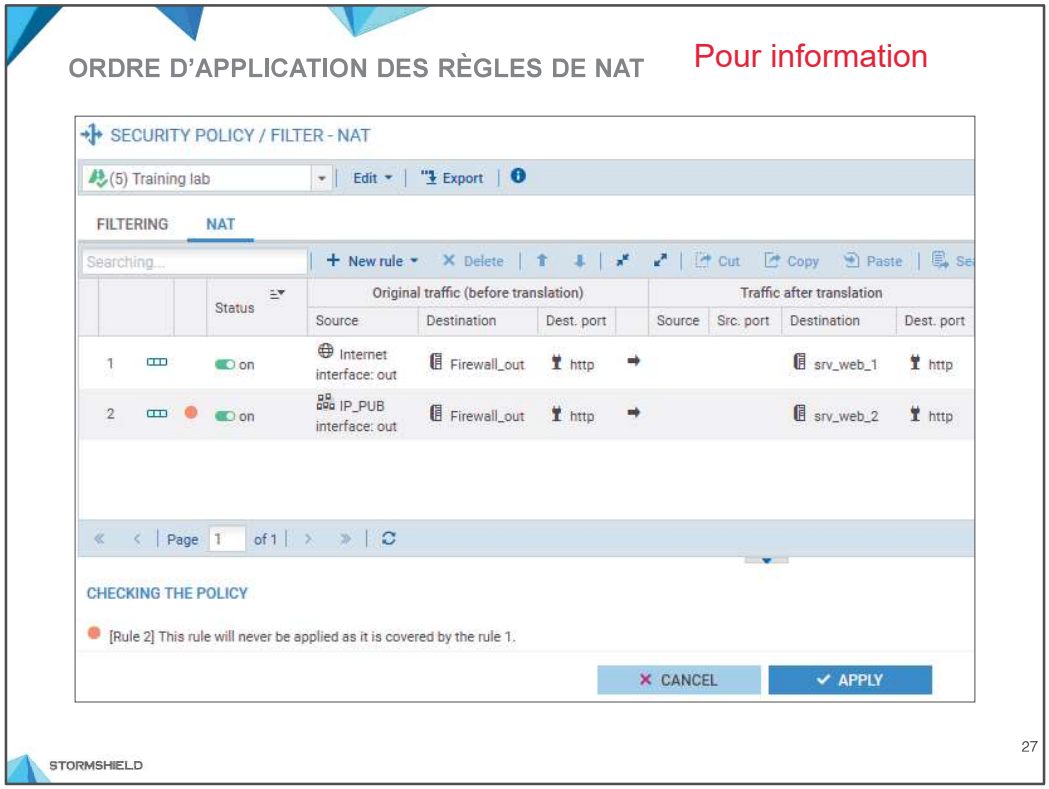


Les règles de NAT statiques sont créées avec **Nouvelle règle ⇒ règle de NAT statique (bimap)** qui lance un assistant pour renseigner les informations suivantes :

- **Machine(s) privée(s)** : L'adresses 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** : Activer la publication ARP pour l'adresse IP publique.

L'exemple illustré dans la figure ci-dessus translate statiquement un serveur SMTP interne identifié par une adresse IP privée **srv_mail_priv** et une adresse IP publique virtuelle dédiée **srv_mail_pub**.

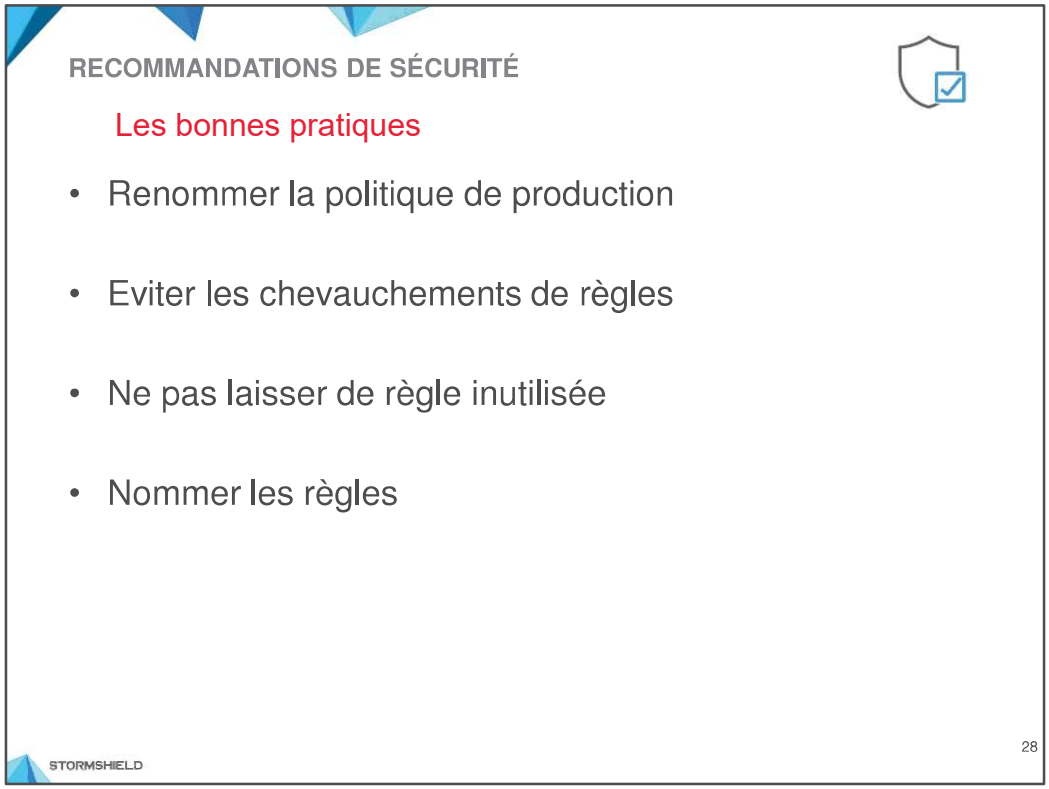
L'assistant ajoute deux règles de translation. La première règle pour la translation du flux sortant du serveur interne vers le réseau public et la deuxième pour le flux entrant à destination de l'adresse IP publique virtuelle. Les deux règles peuvent être modifiées par la suite indépendamment l'une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



L'ordre d'apparition des règles de translation dans la liste est très important, il définit l'ordre dans lequel les nouvelles connexions sont confrontées aux règles de translation. Ainsi, une nouvelle connexion est confrontée aux règles en partant de la première dans la liste jusqu'à la dernière. Dans le cas où la connexion correspond à une règle, la translation définie par cette règle est appliquée et la connexion n'est plus confrontée aux règles suivantes.

Ce principe de fonctionnement peut engendrer une situation de recouvrement si les règles ne sont pas ordonnées d'une manière cohérente. Un exemple est illustré dans la figure ci-dessus, la deuxième règle de translation ne sera jamais utilisée parce qu'elle est recouverte par une règle plus globale située au-dessus dans la liste (Les adresses IP présentes dans le groupe **IP_PUB** sont incluses dans l'objet **Internet**).
Le firewall embarque un moteur de cohérence permettant de détecter ce type de recouvrement qui est signalé à l'administrateur par un message d'alerte affiché en bas de fenêtre.

NOTE : Une solution simple pour cet exemple consiste à inverser l'ordre des deux règles de translation.



Afin de clarifier la lecture des politiques de filtrage, il est recommandé de les nommer explicitement en suivant une convention de nommage précise.

Il est recommandé de ne jamais laisser des règles se recouvrir. Outre l'inutilité le la règle recouverte, cela pourrait mener à laisser des points d'entrés en cas de suppression de la règle couvrante.

Toute règle inutile laisse un point d'entrée potentiel et augmente la surface d'attaque. Elles sont donc à traquer et supprimer régulièrement.

La colonne (par défaut cachée) **nom** permet d'identifier une règle par son nom, c'est un filtre puissant pour rechercher une règle ou pour suivre son comportement en débogage.