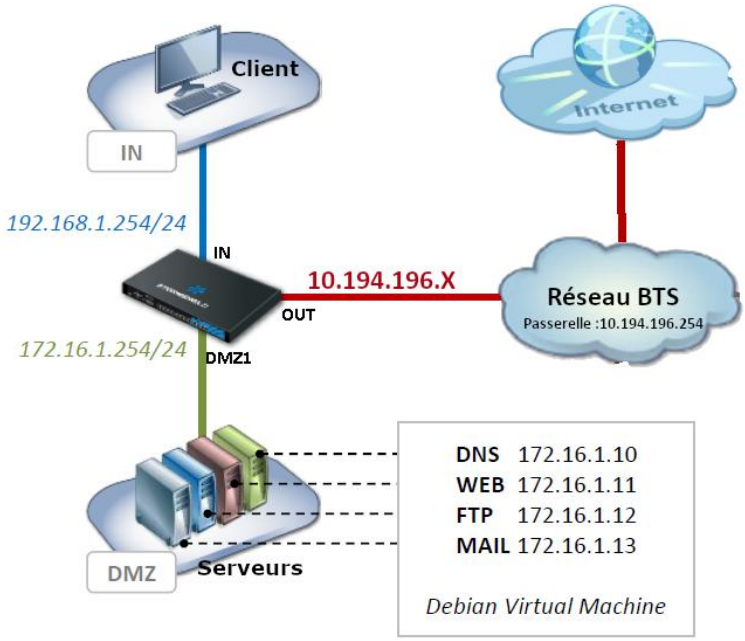
Activité 4 - Stormshield
Translation d'adresses NAT

L'objectif de cette activité est de configurer le filtrage NAT sur le pare-feu Stormshield.

1 – Rappel - Infrastructure virtuelle



Notre structure composée de trois machines virtuelles représente l'architecture réseau d'une entreprise :

- **Un sous réseau 192.168.1.0/24** représente le réseau interne de l'entreprise. Il sera simulé par la VM (Machine Virtuelle) **Client**. Ce sous réseau sera connecté sur l'interface "IN" du pare-feu Stormshield.

- **Un sous réseau "DMZ1" 172.161.0/24** sur lequel on trouve un serveur DNS (172.16.1.10), un serveur WEB (172.16.1.11), un serveur FTP (172.16.1.12) et un serveur mail (172.16.1.13). Il sera simulé par la VM **Serveur**. Ce sous réseau sera connecté sur l'interface "DMZ1" du pare-feu Stormshield.

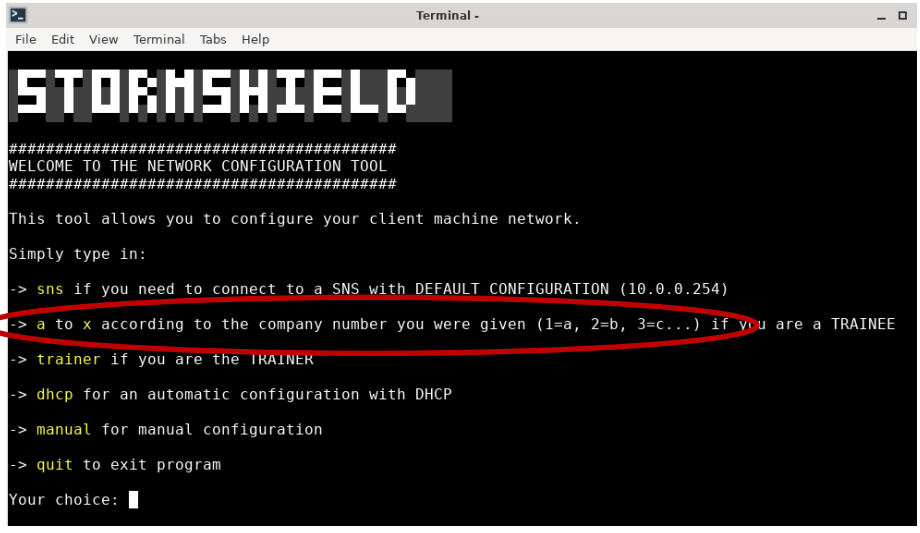
- Le pare feu Stormshield est installé sur une VM nommée **Pare-feu**. **L'interface "OUT" du pare-feu** sera connectée au même réseau que l'hôte sur le réseau 10.194.196.0/24 (Réseau Freebox).

☞ 1 – Démarrez les VM : **Serveur**, **Pare-feu** et **client**.

La VM "**Pare-feu**" démarre avec un Stormshield configuré selon l'activité 3. Son adresse IP est : 192.168.1.254.

Il faut configurer la VM **Client** pour qu'elle soit dans le même réseau que le firewall.

Sélectionnez **"a"** pour configurer la VM **client** dans le réseau 192.168.1.0/24.



☞ 2 – Vérifiez l'adresse IP du client. Si elle est correcte, connectez-vous à l'interface "IN" du firewall.

☞ 3 – Pensez à sélectionner **Entreprise A** au niveau de la VM **Serveurs.**

Le choix "**Entreprise A**" permet de configurer automatiquement les serveurs avec les adresses IP :

- 172.16.1.10 (DNS)
- 172.16.1.11 (WEB)
- 172.16.1.12 (FTP)
- 172.16.1.13 (MAIL)

Votre objectif

Nous considérons que le réseau externe (réseau BTS) est un réseau public dans lequel aucune adresse IP privée n'est tolérée.
Vous devrez mettre en place une translation d'adresses Privées <--> Publiques
L'adresse publique de l'entreprise (**out**) est 10.194.196.x sur l'interface "out". Vous ajouterez deux autres adresses publiques virtuelles (10.194.196.y et 10.194.196.z) qui seront affectées respectivement à vos serveurs FTP et MAIL situés en DMZ.
Retrouvez dans le tableau ci-dessous les adresses correctes pour vos machines.

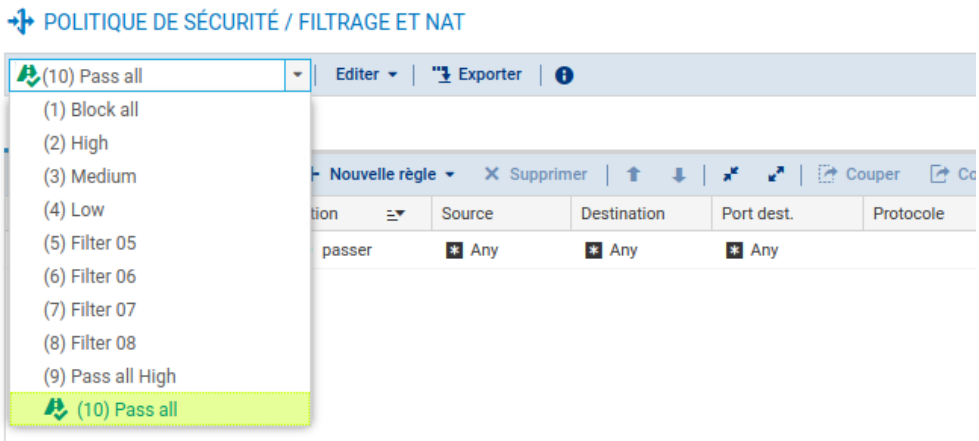
Vous terminerez cette activité en ajoutant une règle NAT afin que les machines de votre réseau interne puissent accéder à vos serveurs en DMZ sans que leur adresse IP privée n'y soit vue.

Etudiant	Adresse IP interface OUT	srv_ftp_pub	srv_mail_pub
1	10.194.196.30	10.194.196.31	10.194.196.32
2	10.194.196.33	10.194.196.34	10.194.196.35
3	10.194.196.36	10.194.196.37	10.194.196.38
4	10.194.196.39	10.194.196.40	10.194.196.41
5	10.194.196.42	10.194.196.43	10.194.196.44
6	10.194.196.45	10.194.196.46	10.194.196.47
7	10.194.196.48	10.194.196.49	10.194.196.50
8	10.194.196.51	10.194.196.52	10.194.196.53
9	10.194.196.54	10.194.196.55	10.194.196.56
10	10.194.196.57	10.194.196.58	10.194.196.59
11	10.194.196.60	10.194.196.61	10.194.196.62
12	10.194.196.63	10.194.196.64	10.194.196.65

Configuration de la politique de sécurité

☞ 4 – Déplacez-vous dans l'interface "Politique de sécurité".

(Menu **Configuration** => **Politique de sécurité** => **Filtrage NAT**)



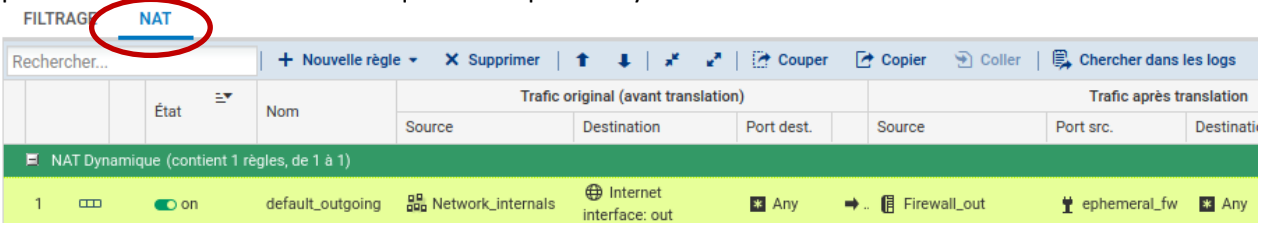
Remarque

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 : 

A la question suivante, vous utiliserez la politique de filtrage n°4 pour mettre en place vos règles. Pour vous faciliter la tâche, vous copierez la politique n°10 sur la n°4 puis vous modifierez les règles.

☞ 5 – Copiez la politique de filtrage/NAT "**(10) Pass all**" vers la politique numéro 4. Renommez la politique numéro 4 "Activite_4" (bouton "**Editer**"). Ensuite, activez cette politique (bouton "**Appliquer**" en bas de la page).

☞ 6 – Cliquez sur l'onglet NAT et ajoutez une règle de NAT afin que les machines de vos réseaux internes puissent accéder à Internet sans que leur IP privée n'y soit vue.



Avant translation

- Source : Network_Internals
- Destination : Internet - Sélectionner "interface OUT" (propriétés avancées)

Après translation

- Source : Firewall_out
- Port Source : ephemeral_fw
- Destination : Any

✍ 7 – Que représente l'objet "Network_Internals" ?

Cet objet représente l'ensemble des réseaux internes connectés aux ports du Stormshield (sauf le port OUT).
L'interface "OUT" est considérée comme un réseau externe.

✍ 8 – Pourquoi utilise-t-on l'objet "**ephemeral_fw**" pour le port source après translation ?

On demande au firewall d'utiliser des ports compris entre 20 000 et 59 999.
Il peut sélectionner un port dans cette plage et l'associer à l'adresse IP du port source.

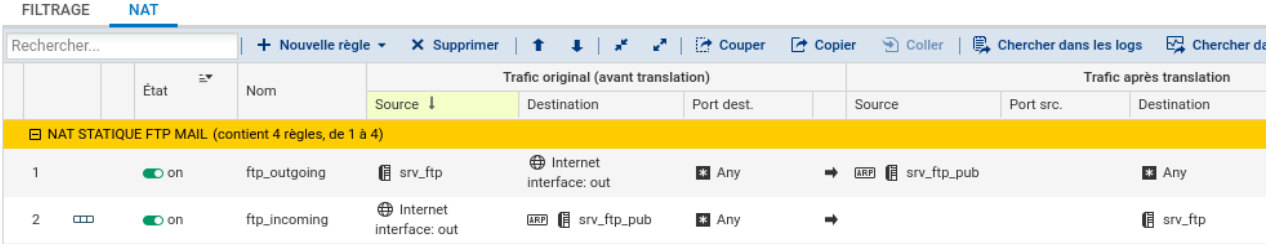
☞ 9 – Pour faciliter la lecture des règles, ajoutez un séparateur "NAT DYNAMIQUE" pour regrouper vos règles (même si dans ce cas, il n'y en a qu'une). N'oubliez de cliquer sur le bouton "Appliquer".

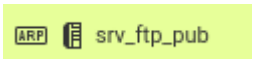
☞ 10 – Testez l'accès à Internet depuis un autre onglet du navigateur de la VM **Cient**.
Vous pouvez tester "**www.mes-cours.fr**".
Si cela ne fonctionne pas, pensez à redémarrer la VM "**serveur**" et sélectionnez "**Entreprise A**".

☞ 11 – L'adresse publique de l'entreprise est 10.194.196.x sur l'interface "out". On aurait pu utiliser cette adresse publique pour nos deux serveurs (FTP – MAIL). Mais on préfère utiliser une adresse spécifique virtuelle pour le serveur FTP et une autre pour le serveur MAIL.

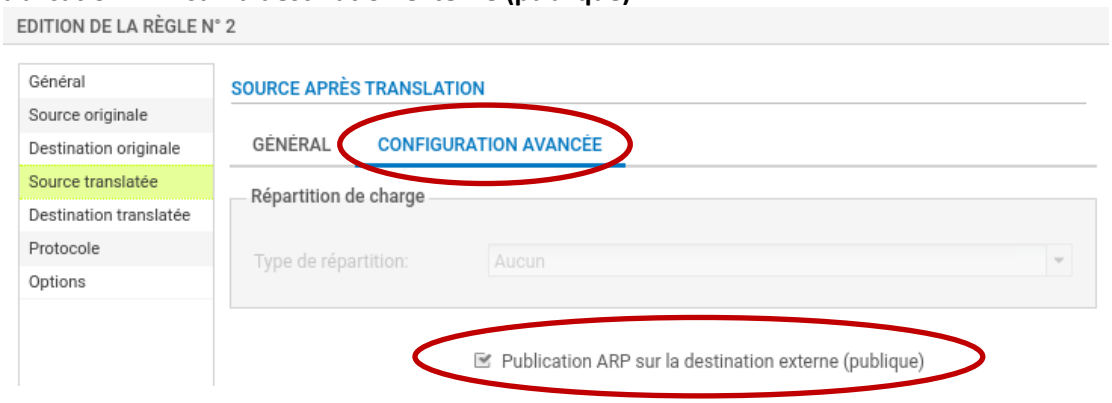
Adresse publique "virtuelle" associée au serveur FTP : 10.194.196.y (srv_ftp_pub).
Adresse publique "virtuelle" associée au serveur MAIL : 10.194.196.z (srv_mail_pub).

Ajoutez les règles de NAT statique qui permettent de joindre chaque serveur depuis le réseau externe grâce à son adresse IP publique.
Voici un exemple pour le serveur FTP, c'est la même chose pour le serveur MAIL.



☞ 12 – Pour faire apparaitre le logo "ARP" 

il faut éditer la règle (double clic) et cocher l'option "**Publication ARP sur la destination externe (publique)**"



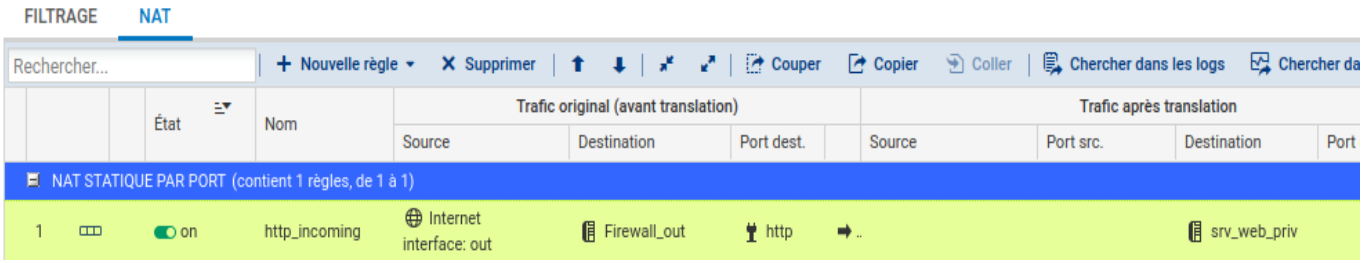
Étant donné que les adresses IP publiques virtuelles ne sont pas configurées sur l'interface externe du firewall, ce dernier ne répondra pas aux requêtes ARP pour la résolution de ces adresses IP en adresse MAC du firewall.

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.

☞ 13 – Ajoutez un séparateur "NAT STATIQUE FTP MAIL" pour regrouper vos règles sur les serveurs FTP et MAIL. Vous devez avoir quatre règles dans ce séparateur.

✍ 14 – Pourquoi a-t-on besoin de deux règles pour le serveur FTP ou pour le serveur MAIL ?
Il faut gérer le trafic FTP sortant et entrant. Une règle par sens de trafic.
Idem pour le serveur MAIL.

☞ 15 – Ajoutez une règle de "NAT statique par port" afin que votre serveur WEB situé en DMZ soit joignable grâce à une redirection de port via l'adresse IP publique portée par votre firewall « 10.194.196.x ».



☞ 16 – Ajoutez un séparateur "NAT STATIQUE PAR PORT".

☞ 17 – Les règles doivent être dans l'ordre suivant :

1 - NAT STATIQUE FTP MAIL
2 - NAT DYNAMIQUE
3 – NAT STATIQUE PAR PORT

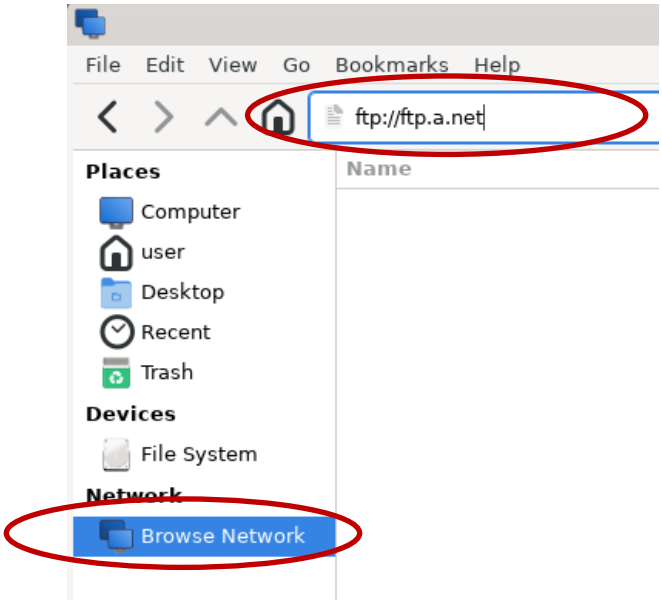
✍ 18 – Notez que la règle de NAT dynamique a été mise après les règles de NAT statiques FTP MAIL. Pourquoi ?
Dans le cas contraire, les serveurs FTP et SMTP souhaitant sortir sur Internet auraient après translation l'IP publique du firewall au lieu de leur IP publique virtuelle dédiée.

☞ 19 –Testez l'accès à Internet. Par exemple testez mes-cours.fr

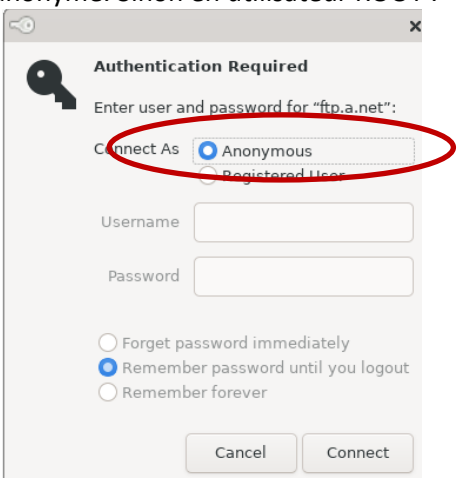
☞ 20 –Testez l'accès au site web local situé dans la DMZ.
Serveur web local : **www.a.net** pour consulter le serveur de l'entreprise.

☞ 21 –Testez l'accès au serveur de messagerie
Serveur Mail : **http://webmail.a.net:808/**
USER ID : **user** Mot de passe : **user**

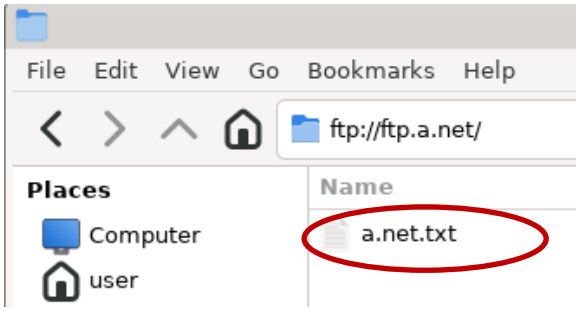
☞ 22 –Testez l'accès au serveur FTP.
Ouvrir l'explorateur de fichier de la VM **Client**. Connectez-vous au serveur FTP. **ftp://ftp.a.net**



Vous pouvez vous connecter en mode anonyme. Sinon en utilisateur ROOT : ID : **root** Mot de passe : **root**



Vous devriez voir le fichier texte **a.net.txt** sur le serveur.

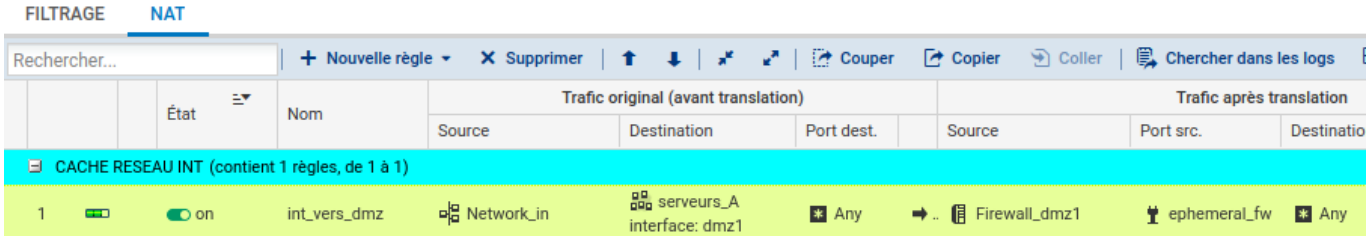


☞ 23 – Suivez cette méthode pour vérifier la règle Statique NAT associée à votre serveur WEB (question 15) :

- Ouvrir un nouvel onglet dans le navigateur de la **machine hôte**.
- Entrez l'adresse http://10.194.196.x Vous devriez être rediriger vers le serveur web situé sur la VM "**serveur**".

☞ 24 – Vous pouvez aussi consulter le site web hébergé sur une autre machine hôte de la salle de TP. Demandez l'adresse IP de l'interface OUT à votre voisin et testez l'accès au site web.

☞ 25 – Ajoutez une règle de NAT afin que les machines de votre réseau interne puissent accéder à vos serveurs en DMZ sans que leur adresse IP privée n'y soit vue.



☞ 26 – Ajoutez un séparateur "CACHE RESEAU INT".

✍ 27 – Quels sont les avantages et inconvénients selon vous de translater les adresses depuis votre réseau interne vers votre DMZ, laquelle est aussi un réseau interne ?

Si vous l'activez, le firewall qui la traite utilisera plus de ressources (table NAT à maintenir), mais un éventuel attaquant ayant pris le contrôle d'un de vos serveurs en DMZ ne pourra pas connaître l'adresse IP du réseau local en capturant les paquets qui en proviennent puisqu'ils sont translatés.

ATTENTION

La règle de NAT permettant d'accéder aux serveurs en DMZ sans que l'IP privée ne soit vue en DMZ sera désactivée ci-dessus, et devra rester désactivée pour la suite des activités.

☞ 28 – Pour suivre l'activité du pare-feu, celui génère un journal accessible dans l'onglet "Monitoring". Cliquez ensuite sur "**Trafic réseau**" ou "**Web**" pour analyser le trafic sur le Stormshield.
Vous devriez retrouver une trace des sites consultés durant ce TP.

Solution :