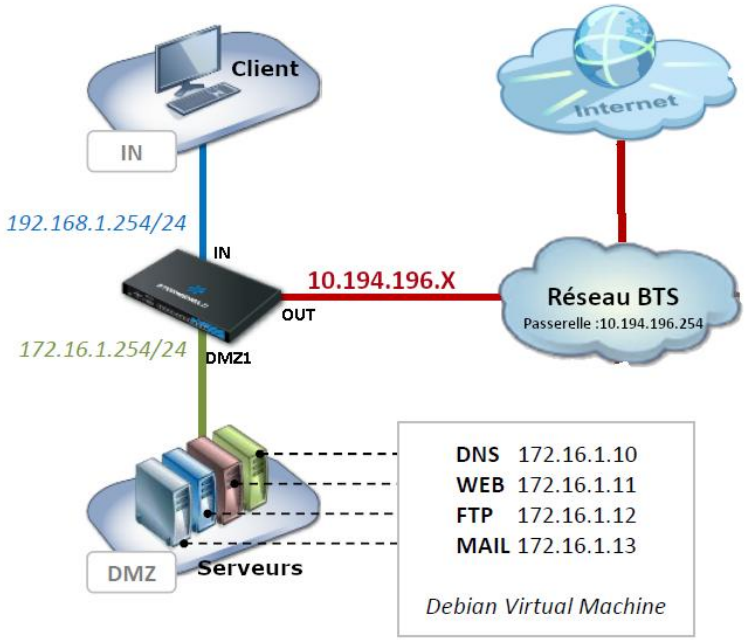
Activité 3
Configuration réseau du pare-feu

L'objectif de cette activité est de mettre en place la configuration réseau du firewall Stormshield.

1 – Rappel - Infrastructure réseau



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).

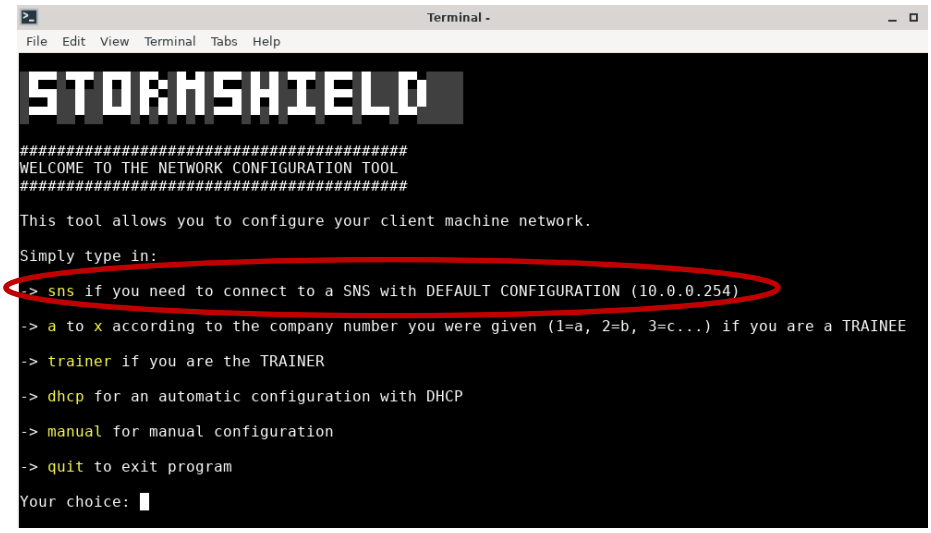
☞ 1 – Démarrez les trois VM de l'entreprise.

La VM **Pare-feu** démarre avec un Stormshield EVA en config usine. Son adresse IP est 10.0.0.254.

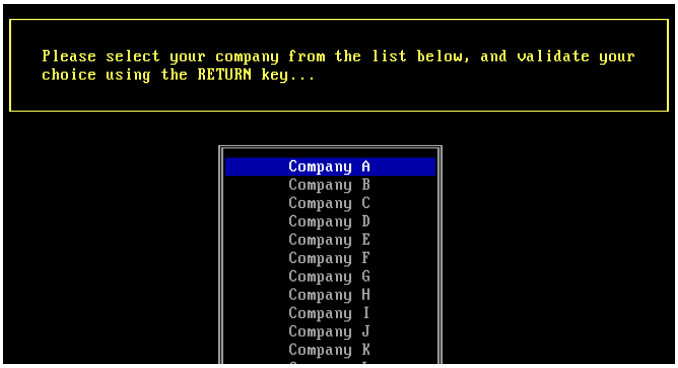
Il faut configurer la VM **Client** pour qu'elle soit dans le même réseau que le firewall.

Ce script permet de configurer rapidement l'adresse IP de votre VM en fonction des activités du TP.

Sélectionnez **sns** pour configurer la VM client dans le réseau 10.0.0.0 /8 (config d'usine du pare-feu).



☞ 2 – 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)

Les objets … pour se faciliter le travail

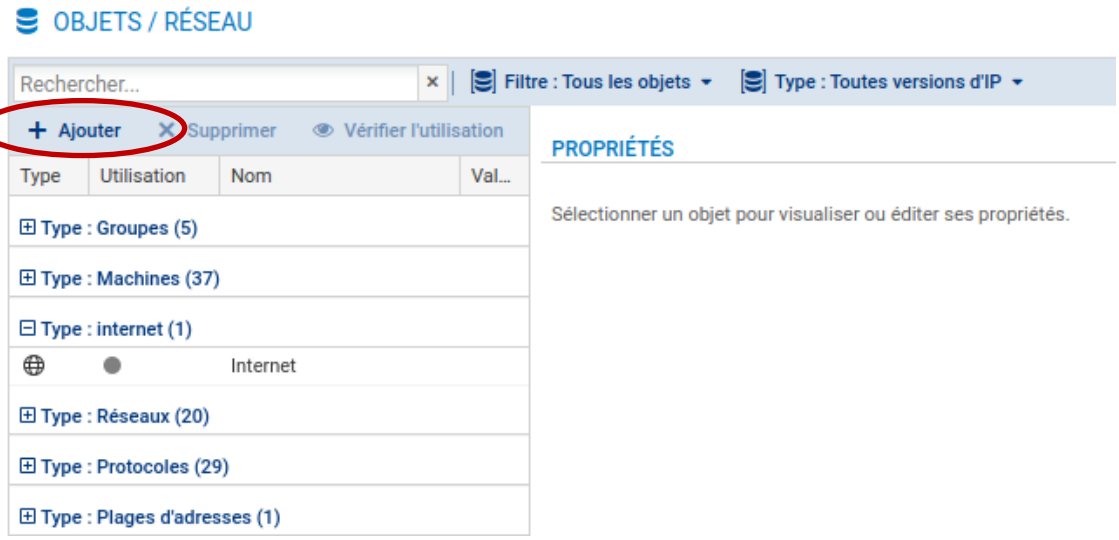
Les menus de configuration des Pare-feu Stormshield utilisent la notion **d'objets.** Un objet représente une valeur (adresse IP, adresse réseau, URL, événement temporel, etc.). L'utilisation d'objets présente deux avantages :

- Cela permet à l'administrateur de manipuler des noms, plus parlants que des valeurs.
- Dans le cas où une valeur change, il suffira de modifier la valeur de l'objet sans se rendre dans tous les menus où l'objet est utilisé.

Par exemple, je peux créer un objet qui contiendra l'adresse IP du pc administrateur :

Nom de l'objet : **pc_admin**
Valeur attribuée : **192.168.1.2**

☞ 2 – Connectez-vous à l'interface du pare-feu. Sélectionnez le menu **Objets** => **Réseau**



Liste des objets machines (host) à créer :

Créez un objet **pc_admin** avec l'adresse **192.168.1.2** (c'est l'adresse IP de la VM **Client**).

Créez un objet **pc_stagiaire** avec l'adresse **192.168.1.200** (on l'utilisera à l'activité 5).

Créez un objet **srv_dns** dont l'adresse IP est **172.16.1.10**

Créez un objet **srv_web** dont l'adresse IP est **172.16.1.11**

Créez un objet **srv_ftp** dont l'adresse IP est **172.16.1.12**

Créez un objet **srv_mail** dont l'adresse IP est **172.16.1.13**

Créez un objet **Gw_default** (passerelle du réseau BTS) dont l'adresse IP est **10.194.196.254**

☞ 3 – Créez un groupe d'objets **serveurs_A** qui contiendra les 4 serveurs : DNS, WEB, FTP et MAIL.

☞ 4 – Ajoutez un objet de type port, nommé **webmail**, associant le protocole **TCP** au port **808**.

Important
L'interface "Out" de votre pare-feu sera connectée au réseau BTS 10.194.196.0/24. Pour éviter un conflit d'adresses entre les différentes interfaces OUT de la salle de TP, veuillez demander une adresse IP fixe unique à votre professeur.
Elle sera comprise dans la plage 10.194.196.30 – 10.194.196.50.

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

☞ 5 – On peut utiliser un fichier CSV pour simplifier la création d'objets. Voici la méthode :
- Dans un premier temps, exportez la base d'objets et analysez la structure du fichier csv.
- Dans un deuxième temps, en vous basant sur le format de ce fichier, créez un autre fichier CSV contenant seulement les deux objets machines :
  - **srv_ftp_pub**: **10.194.196.y**
  - **srv_mail_pub** : **10.194.196.z**

Remplacer "**y**" et "**z**" par l'adresse IP correcte d'après le tableau précédent.

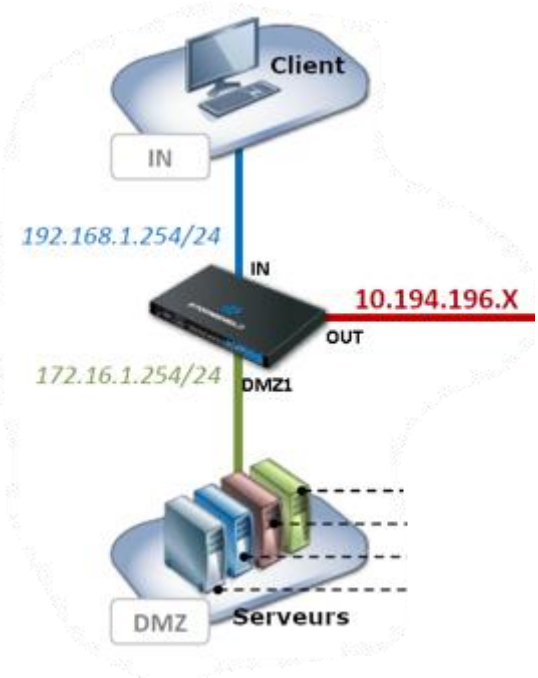
Importez le fichier créé dans la base d'objets réseaux et vérifier la présence des deux objets "srv_ftp_pub" et "srv_mail_pub" dans la base d'objet du pare-feu.

☞ 6 – Vérifiez la présence des deux objets dans la liste des objets machines (host).

Configuration des interfaces du pare-feu

Dans cette partie du TP, vous allez commencer par autoriser tous les trafics traversants ou à destination du firewall. Ensuite, vous allez mettre en place progressivement des restrictions.

☞ 7 - Activer la politique de "**filtrage (10) Pass all"** dans le menu **CONFIGURATION ⇒ POLITIQUE DE SÉCURITÉ ⇒ Filtrage et NAT** qui autorisera tous les trafics traversants ou à destination du firewall.



☞ 6 – Le pare-feu possède trois interfaces : **OUT**, **IN** et **DMZ1**.

La configuration des interfaces s'effectue dans le menu **Configuration** => **Réseau** => **Interfaces.**

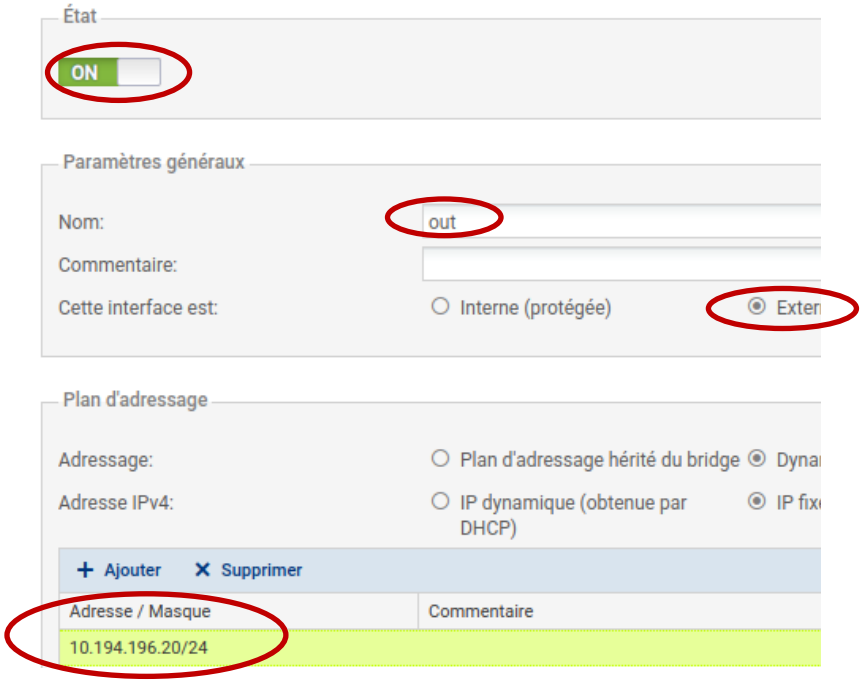
Il faut d'abord sortir les interfaces Ethernet de l'interface bridge (config usine = toutes les interfaces dans le bridge). Cliquez sur l'interface puis déplacez là en dehors du bridge.

Puis, supprimez le bridge.

☞ 8 – Double clic sur l'interface "**OUT**", activez l'interface. Sélectionnez "interface externe".

Puis configurez l'adresse IP : 192.36.253.x/24 (rouge)

(remplacez "x" par la bonne adresse IP).



☞ 9 – Configurez maintenant l'interface "**DMZ1**" :

- Activez l'interface.
- Sélectionnez "**interface interne**".
- Configurez l'adresse IP : 172.16.1.254/24 (vert).

☞ 10 – Configurez maintenant l'interface "**IN**" :

- Activez l'interface
- Sélectionnez "**interface interne**".
- Configurez l'adresse IP : 192.168.1.254/24 (bleu).

Remarque

En config d'usine, le pare-feu est accessible à l'adresse 10.0.0.254 (bridge). Vous venez de supprimer le bridge et de configurer les interfaces OUT, IN et DMZ1.

Vous devez vous reconnecter au pare-feu avec la bonne adresse IP (voir questions 11, 12 et 13).

☞ 11 – Actuellement, la VM **Client** est en 10.0.0.2. Cela correspond à l'adresse IP attribuée par le fichier de configuration (icone **Network Configuration** - option "**sns**"). Vous devez maintenant modifier cette adresse en relançant la configuration réseau mais en sélectionnant l'option "**a**". Cette option configurera votre VM **client** avec une adresse IP dans le réseau 192.168.1.0/24.

✍ 12 – (Vérification) Quelle est l'adresse IP de la VM **Client** ? Est-elle correcte ?
Adresse du type 192.168.1.2 Adresse correcte puisqu'elle est dans le même réseau que celle de l'interface IN.

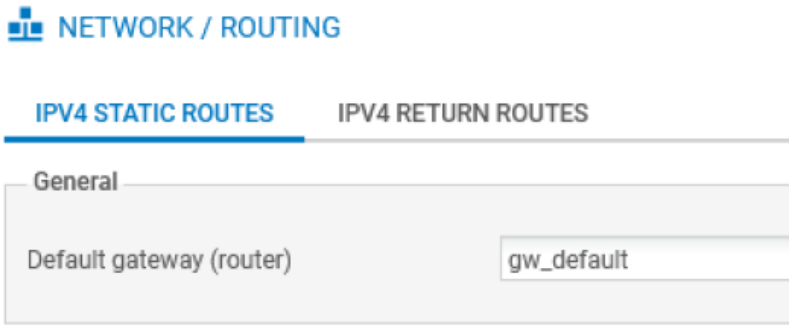
✍ 13 – Quelle adresse IP allez-vous utiliser pour vous connecter à l'interface graphique de pare-feu sachant que vous utilisez le navigateur de la VM **client** ?
On est sur le réseau bleu => adresse de l'interface IN : 192.168.1.254

☞ 14 – Effectuez un ping sur l'interface IN du pare-feu. Si le test est réussi vous pouvez passer à la question suivante. Sinon, dépannez.

☞ 15 – Connectez-vous à l'interface graphique du pare-feu.

✍ 16 – Quelle est l'adresse de la passerelle si la VM **Client** veut accéder à internet ? Quel est le nom de l'objet correspondant que vous avez créé à la question 2 ?
Adresse passerelle : **10.194.196.254** Objet : **Gw_default**
C'est la passerelle du réseau BTS.

☞ 17 – La configuration de la passerelle par défaut s'effectue dans le menu (**Configuration** => **Réseau** => **Routage** => onglet **Routes statiques IPv4**), en sélectionnant le nom de l'objet correspondant à l'adresse IP de la passerelle.



Pensez à effectuer une sauvegarde de votre travail !