Fiche savoirs technologiques : Configuration des Objets Réseau

Dans cette partie, vous allez configurer les objets réseau nécessaires à la mise en place de règles de filtrage et de NAT permettant d'accéder à vos services serveurs en DMZ de l'Agence A à ceux de l'Agence B.

Présentation des Objets

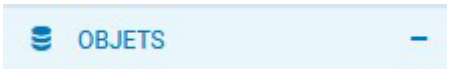
Les menus de configuration des pare-feux Stormshield Network utilisent des objets qui représentent des valeurs (adresse IP, adresse réseau, URL, événement temporel, etc.).

L'utilisation d'objets au lieu de valeurs présente deux avantages majeurs :

- 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 au niveau de l'objet et non dans tous les menus où l'objet est utilisé.

La création et la configuration des objets s'effectuent :

- Dans le menu : **CONFIGURATION / OBJETS**
- Dans le menu raccourci :



- Depuis n'importe quel autre menu via le bouton

Les objets sont classés en 3 catégories :

- 1. **Objets Réseau** : Regroupe tous les objets en relation avec les valeurs réseaux (adresse IP, numéro de port, numéro de protocole, etc.) et les objets temps.
- 2. **Objets Web** : Groupes d'URL (ou groupes de catégories) et groupes de noms de certificats.
- 3. **Certificats et PKI** : Permet la création et la gestion des autorités de certification et de tous les certificats (de type serveur, utilisateur, ou smartcard) qui en découlent.

> Cette activité concerne principalement aux objets réseaux :
>
> - Les objets Web seront abordés dans l'activité **Filtrage applicatif** ;
> - Les objets Certificats et PKI seront abordés dans le chapitre **PKI**.

Lors de la création de la passerelle par défaut, vous avez créé l'**objet Machine GW_NatNetwork**.

La syntaxe des noms des objets doit respecter quelques restrictions définies dans le tableau ci-dessous. De plus, elle est insensible à la casse.

Recommandations :

- suivre une convention de nommage des objets,
- limiter l'usage des objets dynamiques ;
- limiter le nombre d'objets inutilisés ;
- utiliser un groupe d'objet d'administration contenant l'ensemble des IP et des réseaux d'administration permet de réutiliser ce groupe dans toutes les règles de filtrage liées à l'administration et donc de maintenir leur cohérence tout en facilitant leur modification ;
- **éviter les doublons**. C'est une source d'erreur courante lors de la modification de règles de filtrage. On se retrouve dans un cas où la modification d'un objet n'impacte pas toutes les règles qui auraient dû l'être, créant ainsi des trous dans la sécurité.

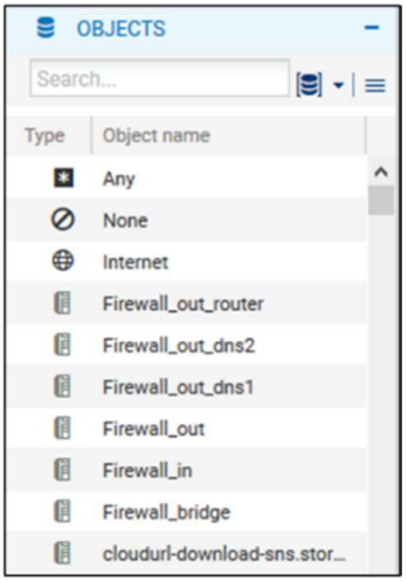
On peut distinguer deux types d'objets particuliers en plus des objets qui peuvent être créés par l'administrateur :

- **Objets implicites** : Ils sont créés automatiquement par le firewall et dépendent de la configuration réseau. Ces objets sont en lecture seule et ne peuvent être ni modifiés ni supprimés par l'administrateur. Par exemple, l'objet **Firewall_out**, est créé automatiquement lorsqu'une adresse IP est associée à l'interface **OUT**. L'objet **Network_internals** regroupe tous les réseaux accessibles via les interfaces internes.
- **Objets préconfigurés** : Ils sont présents par défaut dans la liste des objets. Ils représentent des valeurs de paramètres réseaux standardisées (ports, protocoles, réseaux) et des valeurs nécessaires pour le fonctionnement du firewall (adresse IP des serveurs Stormshield pour les mises à jour). On trouvera par exemple le protocole ICMP et l'objet **Internet**. Ce dernier regroupe l'ensemble

des machines ne faisant pas partie des réseaux internes.

> Il est **conseillé** d'utiliser les objets **implicites et préconfigurés** et d'éviter de créer d'autres objets portant les mêmes valeurs.

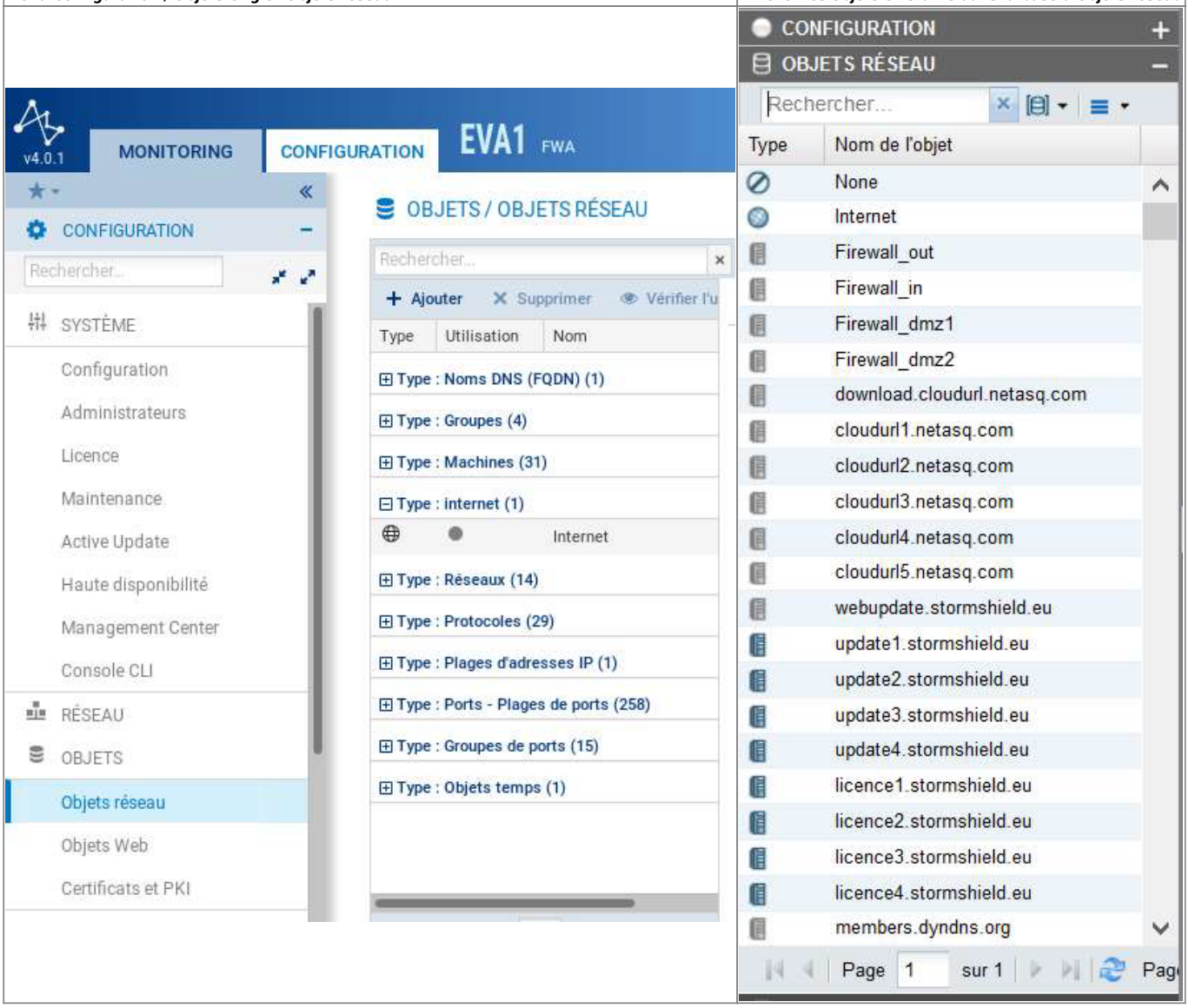
Préfixes interdits	Caractères interdis dans le nom	Noms d'objets interdis	Caractères interdits dans la description
firewall_	<tabulation>	Any	<tabulation>
Network_	<espace>	None	#
Ephemeral_	!	Anonymous	@
Global_	"	Broadcast	"
Vlan_	#	Internet	
Bridge_	,		
	=		
	@		
	[		
	]		
	\		



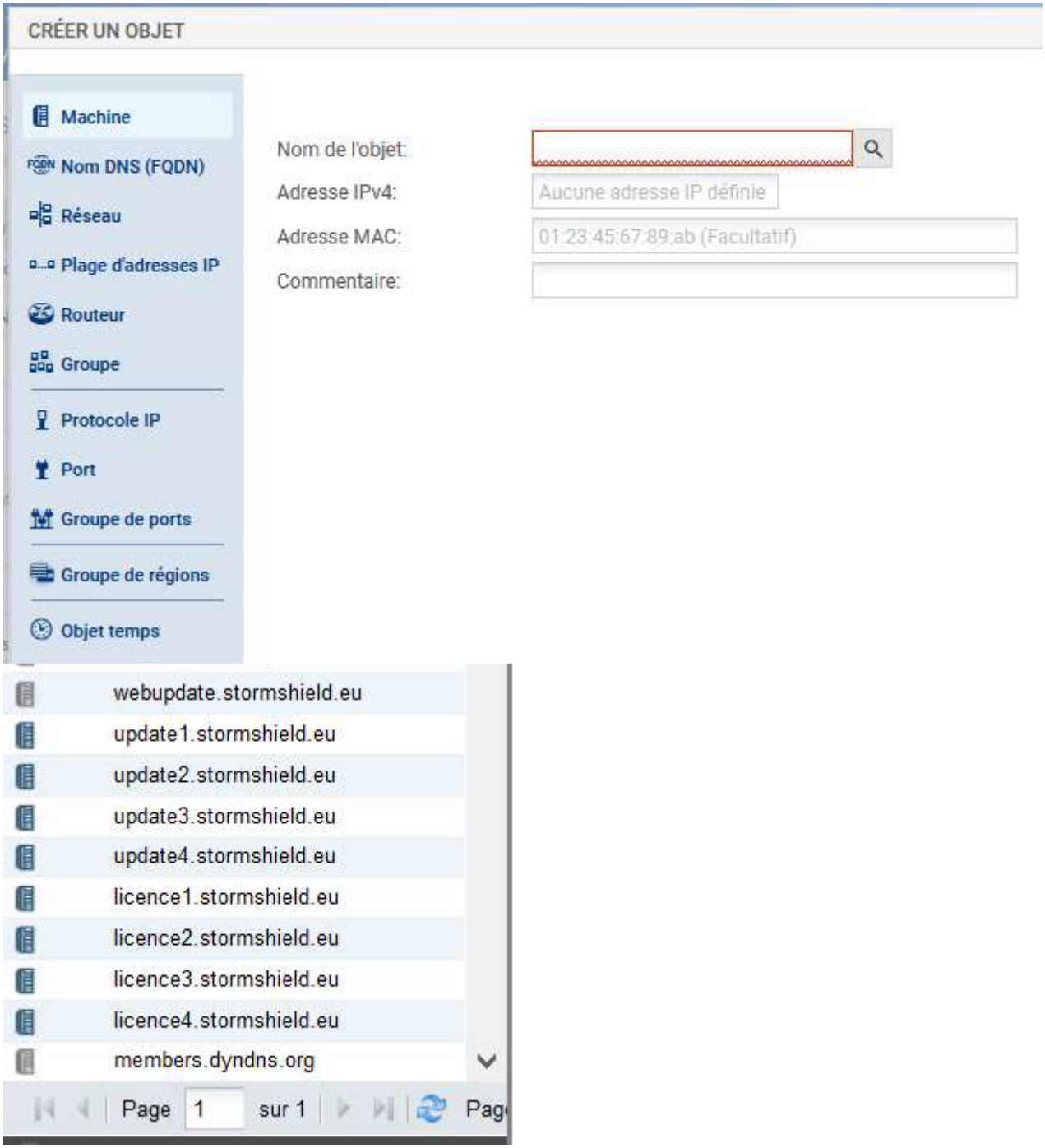
Création des Objets Réseaux

Le menu **Configuration** / **Objets** onglet **Objets réseau** ou le menu **Objets réseau** permettent de visualiser les objets, de les modifier ou d'en ajouter.

Menu Configuration / Objets Onglet Objets réseaux	Afficher les objets existants dans la base d'objets réseau



- Ouvrez **Configuration** / **Objets** / **Objets réseau** et cliquez le bouton **Ajouter** pour ajouter les objets souhaités.



Les types d'objets suivants peuvent être créés :

- **Machine** : Une adresse IP,
- **Nom DNS (FQDN)** : Toutes les adresses IP associées à un nom FQDN par résolution DNS,
- **Réseau** : Une adresse réseau,
- **Plage d'adresses IP** : Une plage d'adresses,
- **Routeur** : Permet de renseigner une ou plusieurs passerelles pour un routage par répartition de charge avec ou sans passerelle de secours.
- **Groupe** : Un groupe d'objets portant une ou plusieurs adresses IP : machines, plages d'adresses IP, réseaux ou d'autres groupes,
- **Protocole IP** : l'ID du protocole au niveau IP,
- **Port - Plage de ports** : Un port ou une plage de ports. Il/Elle peut être limité(e) à un protocole de transport particulier (TCP ou UDP),
- **Groupe de ports** : Un groupe d'objets portant des ports ou des plages de ports, ainsi que d'autres groupes de ports,
- **Groupe de régions** : Un groupe de pays ou de continents. Ce type d'objet peut être utilisé dans la géolocalisation des adresses IP,
- **Objet temps** : Un événement temporel (ponctuel, jour de l'année, jour(s) de la semaine ou plage(s) horaire(s)).

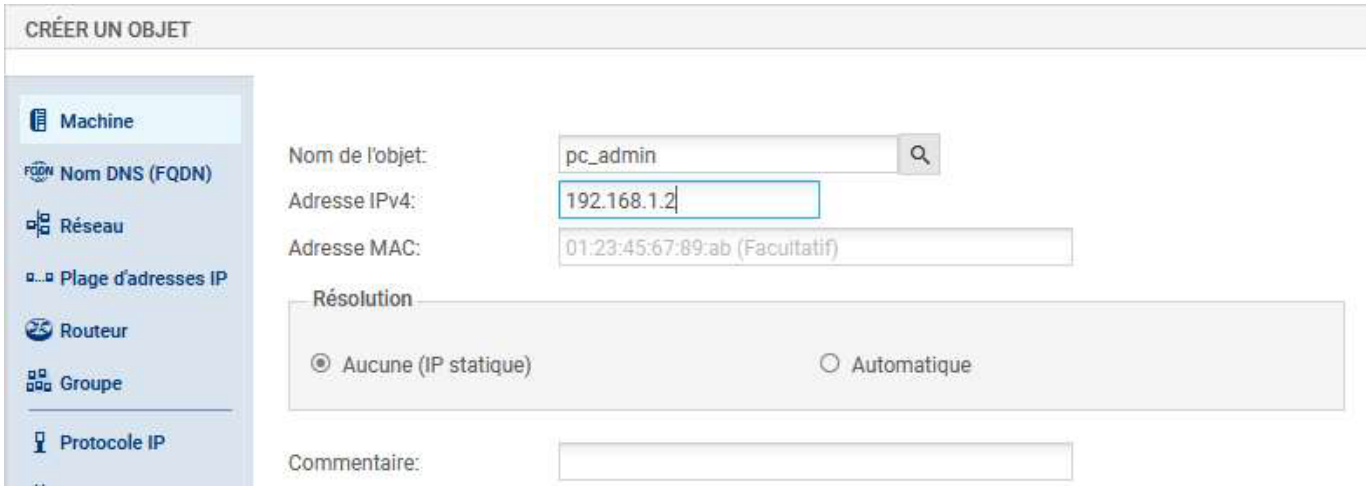
Utilisez un typage d'objets adéquat (objet réseau pour les réseaux, objet machine pour les pare-feux, etc.).

Rappel : Dans ce qui suit, le « x » correspond à l'agence considérée, A⇒1, B⇒2, C⇒3, D⇒4, etc.

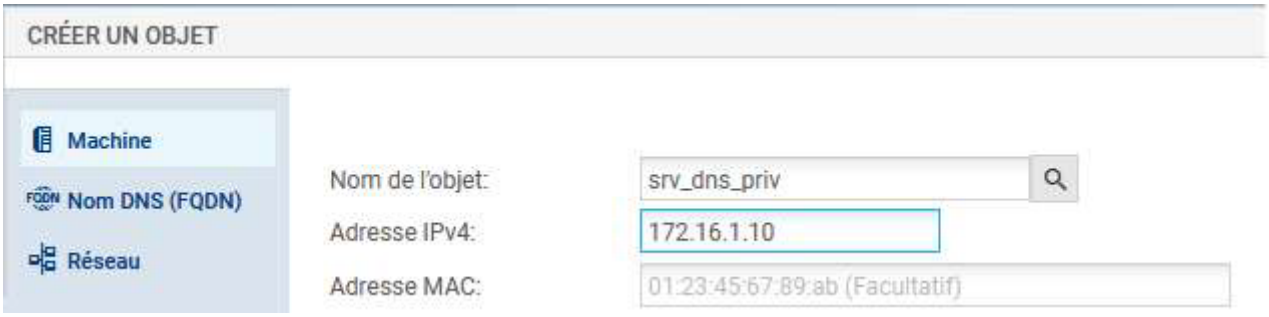
Créer des Objets Machines et Réseaux

Vous allez maintenant créer les objets correspondants à vos machines et réseaux internes.

- Créez un objet **Machine** de nom **pc_admin** avec l'adresse IP **192.168.x.2**
- Dans **Configuration / Objets / Objets réseau** cliquez le bouton **Ajouter** et saisissez les valeurs ci-dessous puis cliquez **Créer** :

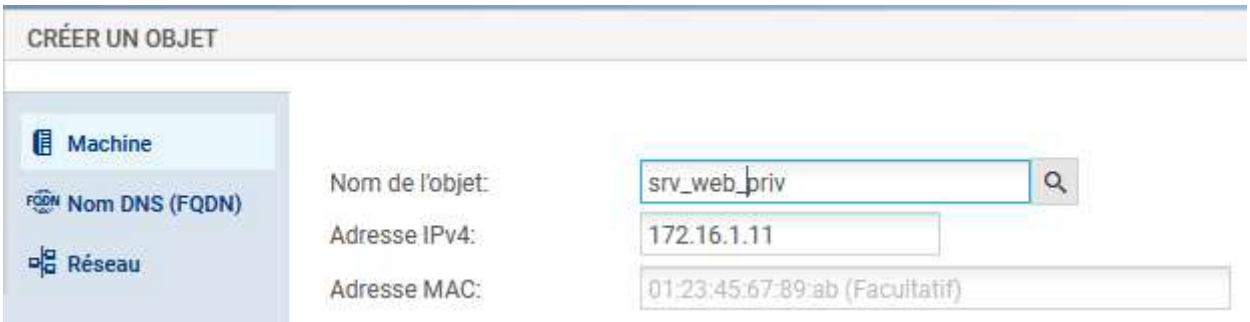


- Créez un objet **srv_dns_priv** dont l'adresse IP est **172.16.x.10**

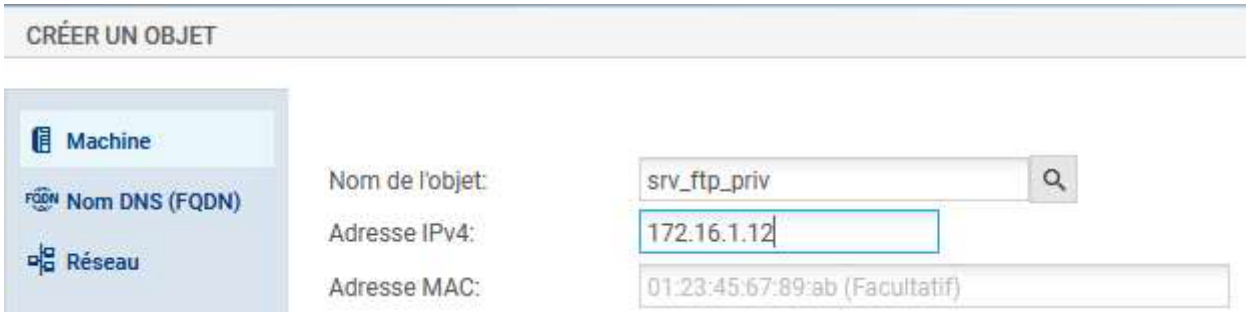


Vous pouvez utiliser le bouton **Créer et dupliquer** pour la création des objets de même type.

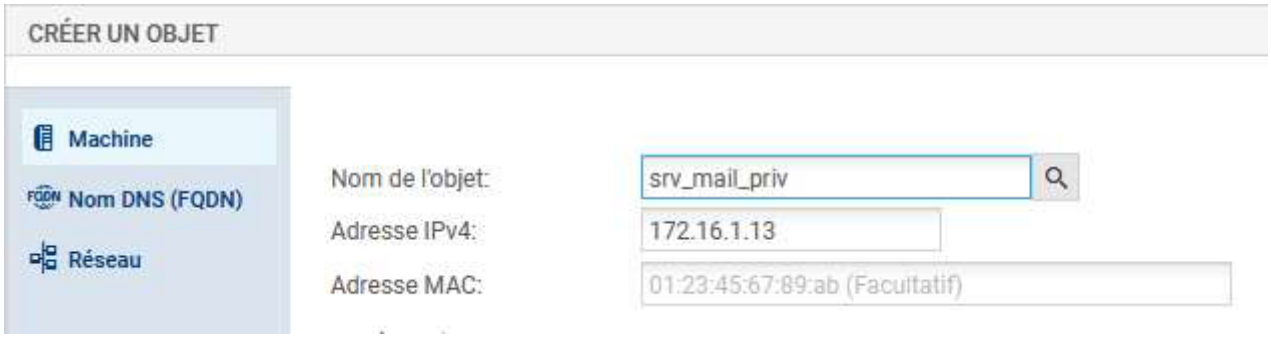
- Créez un objet **srv_web_priv** dont l'adresse IP est **172.16.x.11**



- Créez un objet **srv_ftp_priv** dont l'adresse IP est **172.16.x.12**



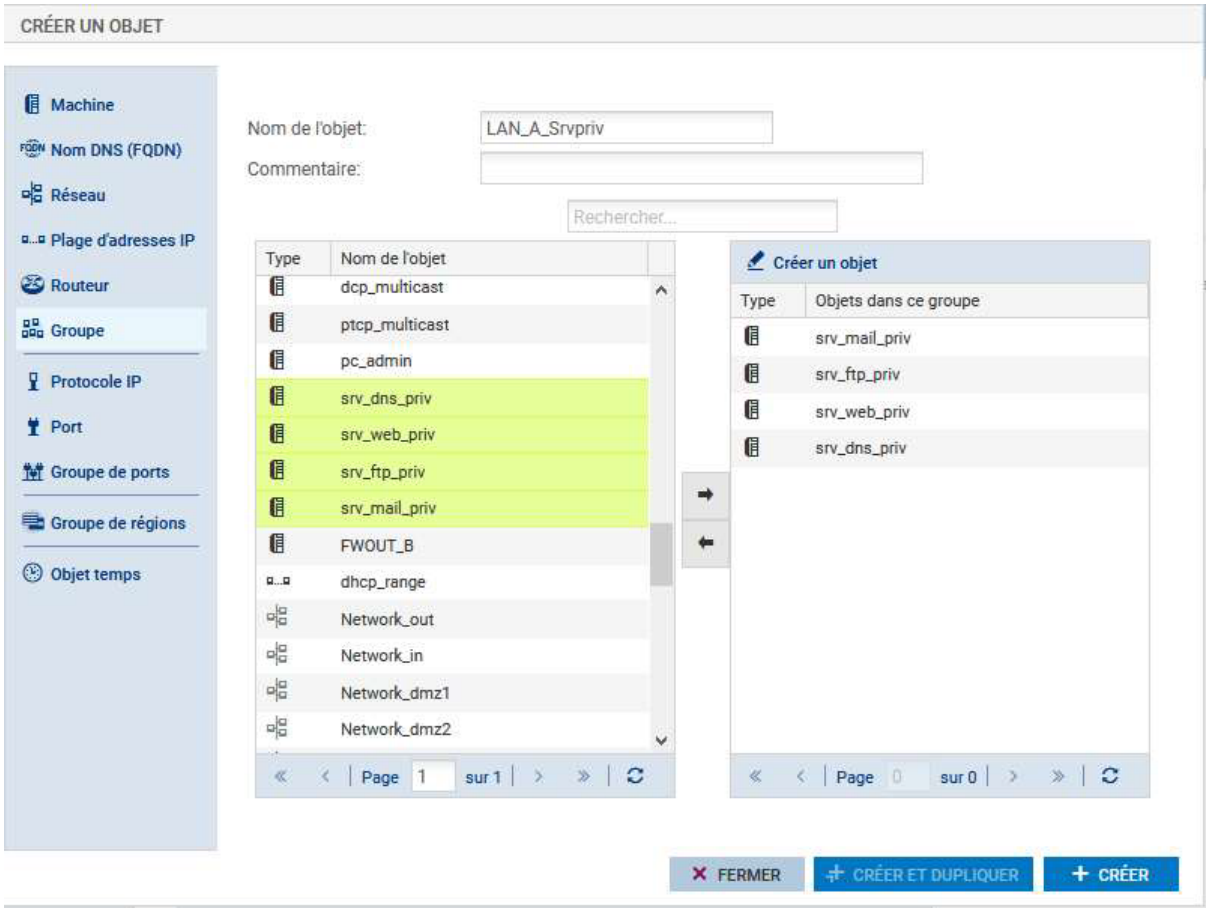
- Créez un objet **srv_mail_priv** dont l'adresse IP est **172.16.x.13**



Cliquez la liste **Type : Machines** pour déplier et visualiser son contenu. Vous devez avoir à la fin de la liste des objets **Machines**, les nouveaux objets créés :

		FWOUT_Siege	192.36.253.1 / static
		FWOUT_B	192.36.253.20 / static
		pc_admin	192.168.1.2 / static
		srv_dns_priv	172.16.1.10 / static
		srv_web_priv	172.16.1.11 / static
		srv_ftp_priv	172.16.1.12 / static
		srv_mail_priv	172.16.1.13 / static

- Créez un groupe d'objets qui contiendra les 4 serveurs que vous venez de définir de nom **LAN_A_Srvpriv**
  - Cliquez **Ajouter** puis **Groupe** ;
  - dans la zone **Nom de l'objet** saisissez **LAN_A_Srvpriv** ;
  - sélectionnez les 4 objets serveurs et à l'aide de la flèche déplacez les dans la zone de droite **Objets dans ce groupe**
    - puis cliquez sur **Créer**.



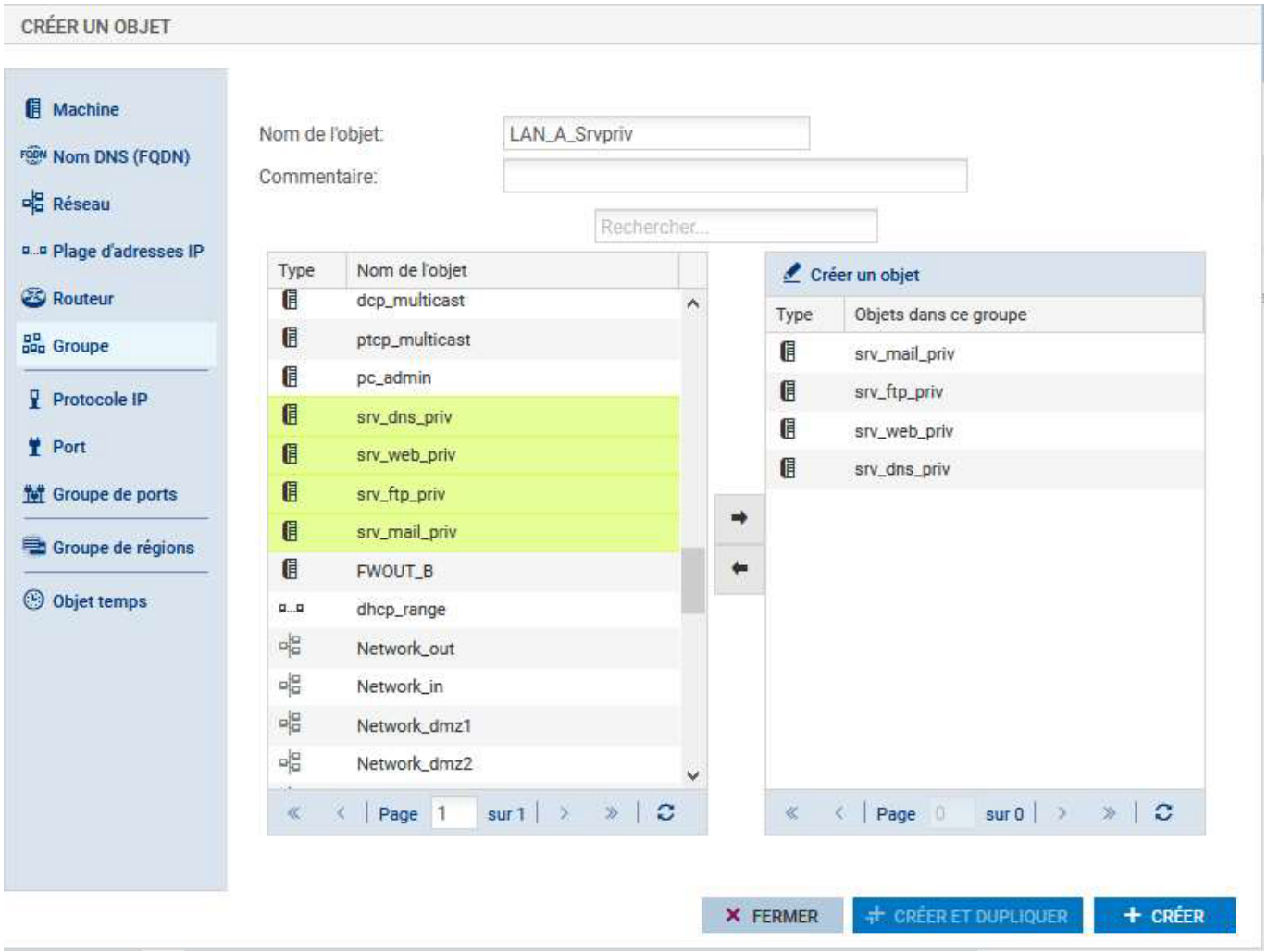
En suivant le même procédé, **créez les objets machines et réseaux** pour la deuxième agence :

- Firewalls distants (adresse des interfaces externes) ; exemple : **FWOUT_x** en 192.36.253.x0 ;
- Réseaux distants (adresse des réseaux internes) ; exemple : **LAN_x** en 192.168.x.0 / 255.255.255.0 ;
- Réseau DMZ distant du siège : **DMZ_x** en 172.16.x.0 / 255.255.255.0

Créer un objet Port

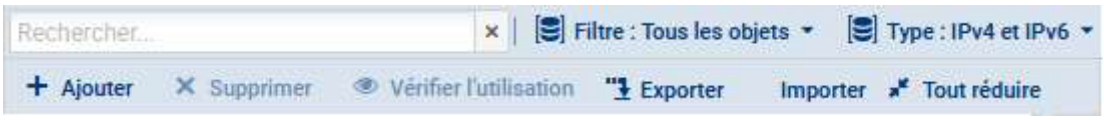
Ajoutez un nouvel objet **Port** basé sur TCP fonctionnant sur le port **808** appelé **webmail**

- Cliquez le bouton **Ajouter Port** ;
- choisir le type **Port** ;
- Nom de l'objet : **webmail** ;
- Port : **808**, Protocole : **TCP** ;
- puis cliquez le bouton **Créer**.



Import/Export des Objets Réseaux

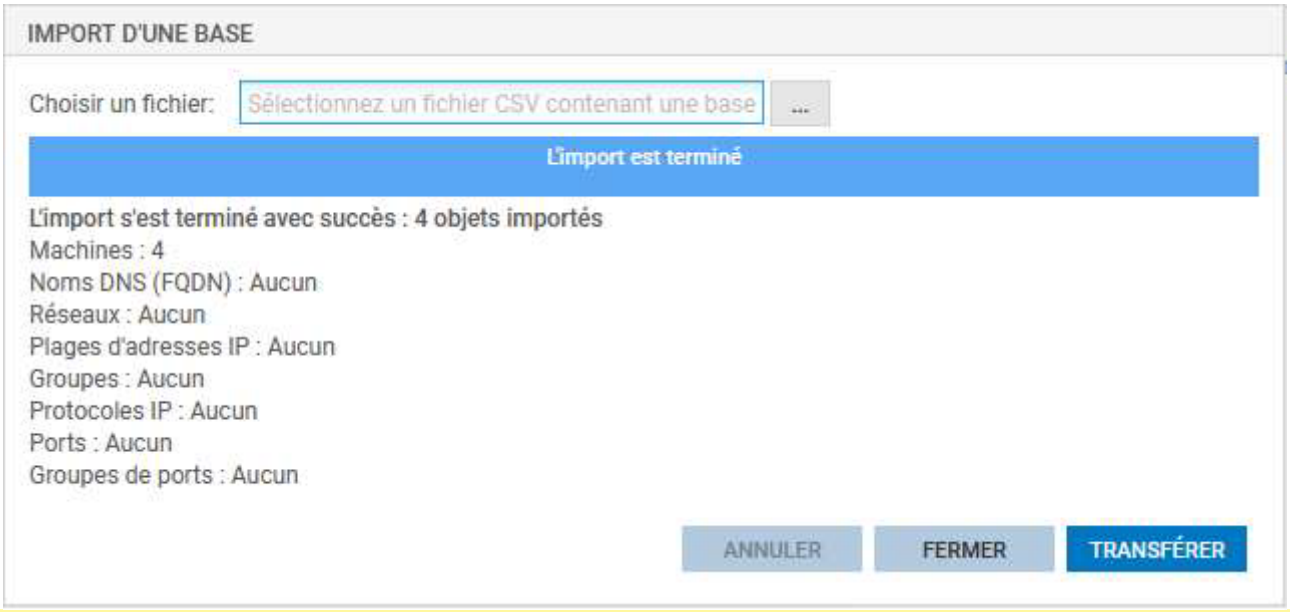
Vous allez utiliser les boutons **Exporter et Importer** pour modifier la base d'objets depuis un fichier csv.



- Cliquez **Exporter** pour exporter la base d'objets précédemment créés dans un fichier CSV ;
- En vous basant sur le format de ce fichier, créez un autre fichier CSV **ObjetsSNSPub.csv** contenant quatre nouveaux objets machines correspondant à l'adresse publique de vos serveurs privés :
  - **srv_dns_pub** : adresse IP **192.36.253.x0** ;
  - **srv_web_pub** : adresse IP **192.36.253.x1** ;
  - **srv_ftp_pub** : adresse IP **192.36.253.x2** ;
  - **srv_mail_pub** : adresse IP **192.36.253.x3**.

Vous allez importer le fichier CSV dans la base d'objets réseaux.

- Cliquez **Importer** puis choisissez le fichier **ObjetsSNSPub.csv** ;
- cliquez **Transférer**
- puis **Fermer**.



Note : En cas de problème à l'importation, encodez le fichier en **UTF-8** avec des retours à la ligne type **Unix (LF)**.

Vous devez avoir les nouveaux objets machine dans la liste :

- Copiez le fichier CSV ver un nouveau fichier **ObjetsSNSPub_X.csv**, remplacez les noms et les adresses IP par les adresses IP publiques des machines de l'autre agence :
  - ***srv_dns_pubX : adresse IP 192.36.253.y0 * srv_web_pubX : adresse IP 192.36.253.y1 * srv_ftp_pubX : adresse IP 192.36.253.y2 * srv_mail_pub_X : adresse IP 192.36.253.y3 * Cliquez Importer, puis choisissez le fichier ObjetsSNSPub_X.csv, cliquez Transférer* puis Fermer.***

Les objets ainsi créés seront utilisés dans les règles de filtrage et de NAT.

===== Retour Accueil Stormshield ===== * Stormshield