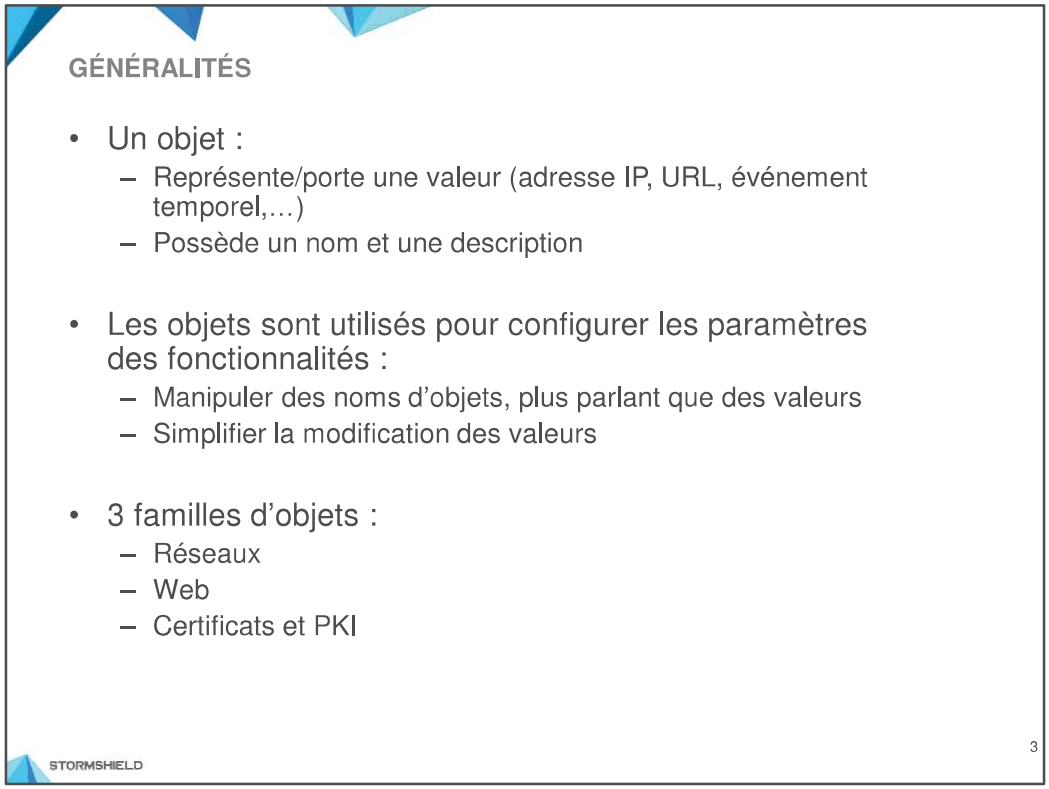


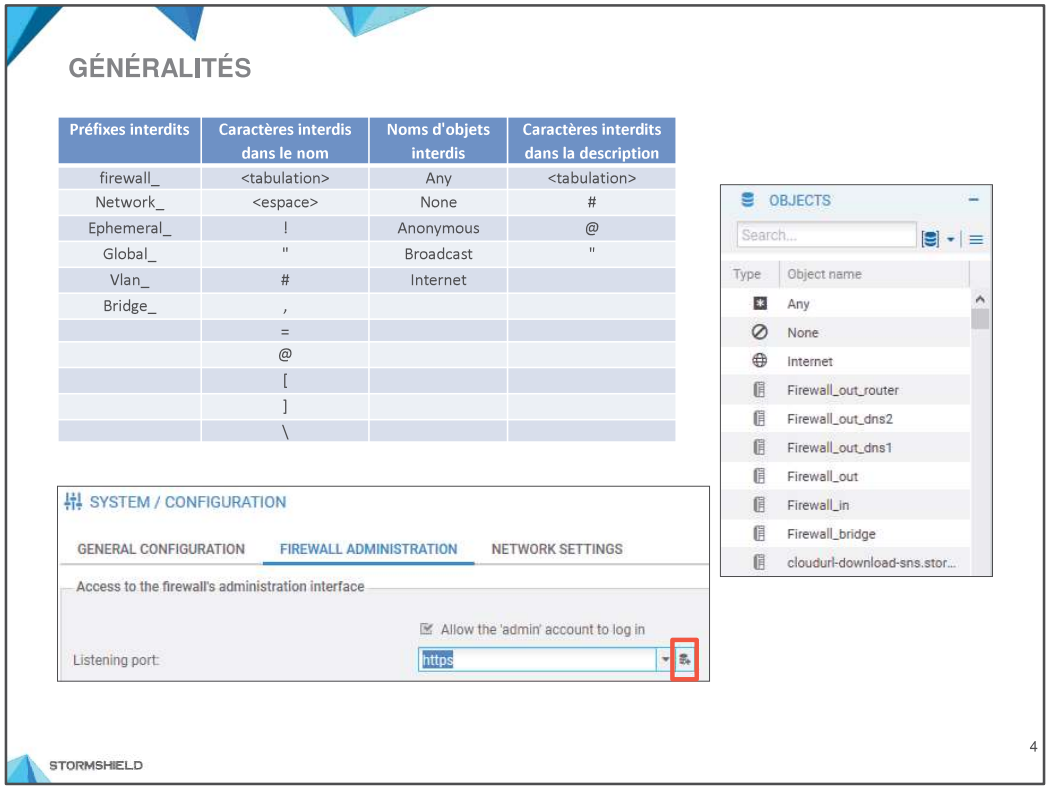
Les menus de configuration des firewalls Stormshield Network utilisent la notion d'objets qui représentent des valeurs (adresse IP, adresse réseau, URL, événement temporel, etc.). L'utilisation d'objets au lieu de valeurs présente deux avantages majeurs :

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

Les objets sont classés en 3 familles :

1. **Objets Réseaux :** 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 toutes les identités (de type serveur, utilisateur, ou smartcard) qui en découlent.

Dans ce module, nous nous intéresserons principalement aux objets réseaux. Les objets Web seront abordés dans le module « protection applicative ». La partie Certificats et PKI est, quant à elle, abordée dans la formation CSNE.

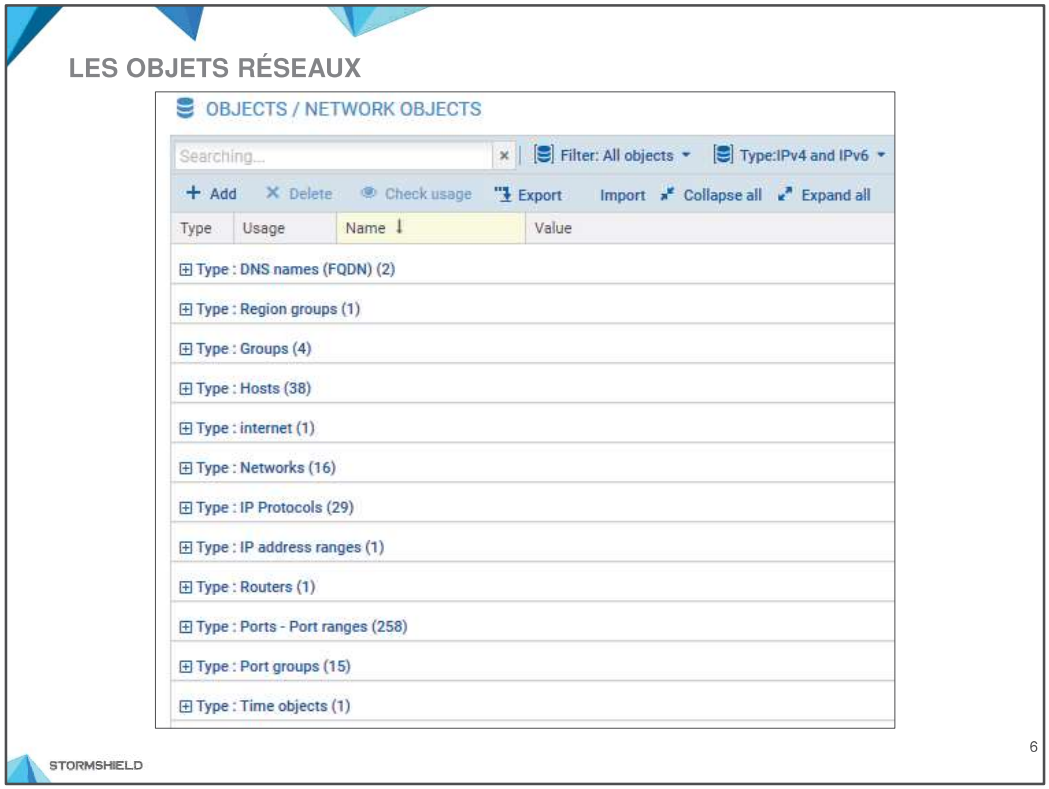


La syntaxe des noms des objets doit respecter quelques restrictions définies dans le tableau ci-dessus. De plus, elle est insensible à la casse.

La création et la configuration des objets s'effectuent :

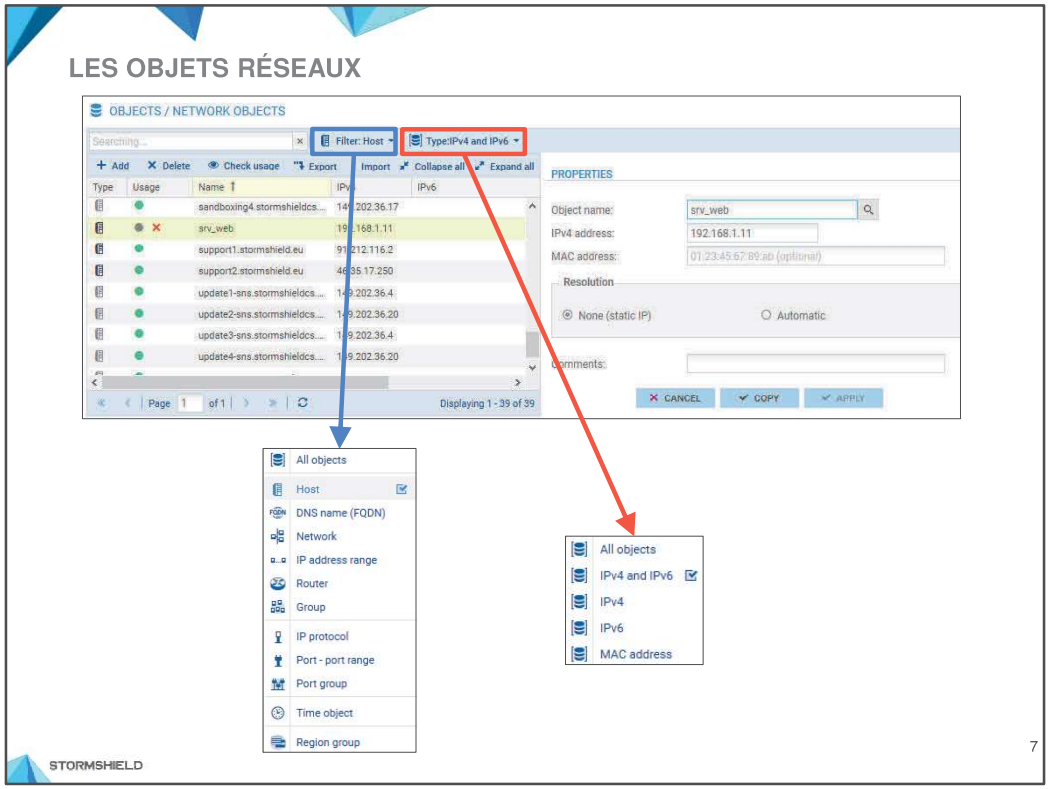
- Dans le menu : **CONFIGURATION ⇒ OBJETS**
- Dans le menu : **OBJETS**
- Depuis n'importe quel autre menu via le bouton encadré dans la diapositive ci-dessus (création contextuelle).

NOTE : Il est possible de créer plusieurs objets portant la même valeur. Cependant, nous vous déconseillons de le faire afin de simplifier la lecture des menus de configuration (principalement les règles de filtrage/NAT) et des bases d'objets. Et également, afin de faciliter leur maintenance.



La base d'objets réseaux est accessible depuis le menu **CONFIGURATION ⇒ OBJETS ⇒ Objets réseaux**. Elle comprend les catégories d'objets suivants :

- **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
- **Port – Plage de ports** : Un port ou une plage de port. Il/Elle peut être limité(e) à un protocole de transport particulier (TCP ou UDP),
- **Protocole IP** : l'ID du protocole au niveau IP,
- **Groupe** : Un groupe d'objets portant une ou plusieurs adresses IP : machines, plages d'adresses IP, réseaux ou d'autres groupes,
- **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,
- **Routeur** : Permet de renseigner une ou plusieurs passerelles pour un routage par répartition de charge avec ou sans passerelle de secours. Cet objet sera détaillé dans la partie Routage du module Configuration Réseau,
- **Temps** : Un événement temporel (ponctuel, jour de l'année, jour(s) de la semaine ou plage(s) horaire(s)).

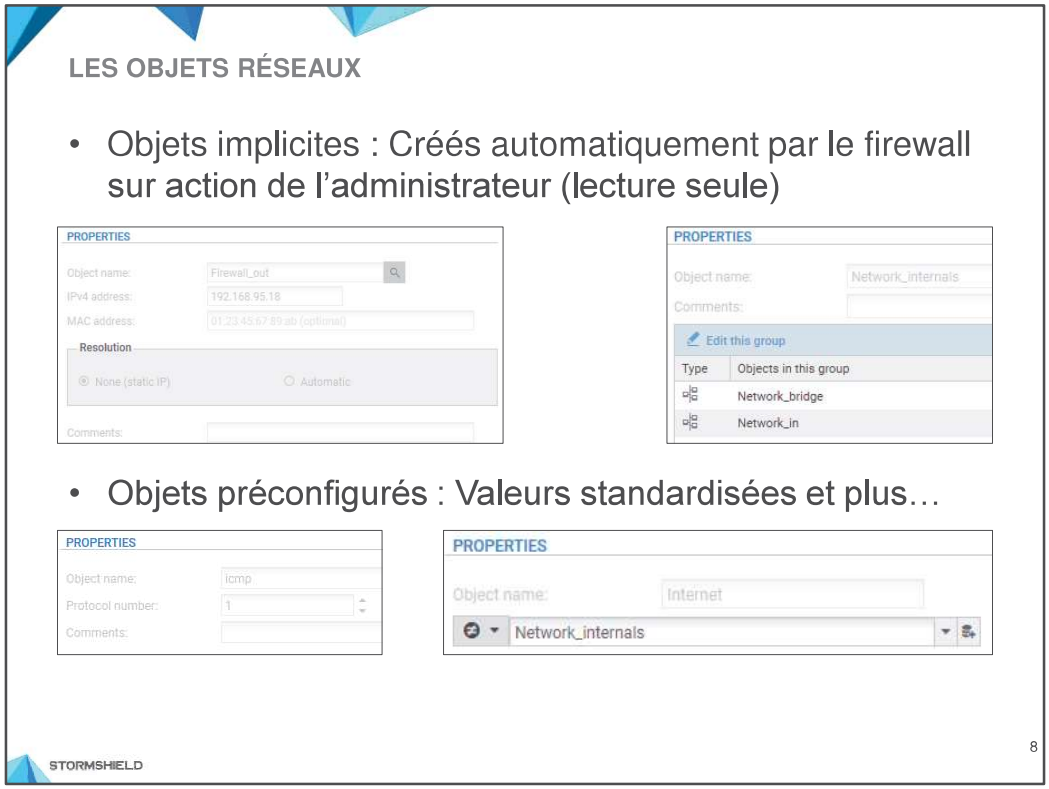


Le menu **CONFIGURATION ⇒ OBJETS ⇒ Objets réseaux** offre plusieurs fonctionnalités pour gérer les objets réseaux :

- **Barre de recherche :** Effectuer une recherche sur le nom, le commentaire ou la valeur de l'objet.
- **Filtre :** Filtrer l'affichage des objets en fonction de leur catégorie (machine, réseau, port, etc.).
- **Type :** Filtrer l'affichage des objets en fonction du type d'adresse utilisé (double pile, IPv4, IPv6, adresse MAC).
- **Ajouter :** Créer un nouvel objet.
- **Supprimer :** Supprimer un objet sélectionné. Si celui-ci est utilisé dans une configuration, une fenêtre s'affichera pour vous permettre de vérifier le module dans lequel l'objet est utilisé, forcer la suppression ou annuler la suppression.
- **Vérifier l'utilisation :** Affiche dans le bandeau de gauche le ou les menus dans lesquels l'objet sélectionné est utilisé.
- **Exporter** : Exporter la base d'objets réseaux dans un fichier CSV.
- **Importer** : Importer des objets à partir d'un fichier CSV.

Le reste du menu est composé de deux parties :

- **Liste des objets :** Affiche tous les objets réseaux organisés selon les filtres d'affichage utilisés. Chaque objet est affiché sur une ligne avec les informations suivantes :
  - La catégorie de l'objet représenté par une icône,
  - L'utilisation : vert signifie que l'objet est utilisé et gris le contraire,
  - Le nom de l'objet,
  - La valeur portée par l'objet.
- **Propriétés :** Affiche les attributs de l'objet sélectionné. Leur modification s'effectue depuis cet encadré.

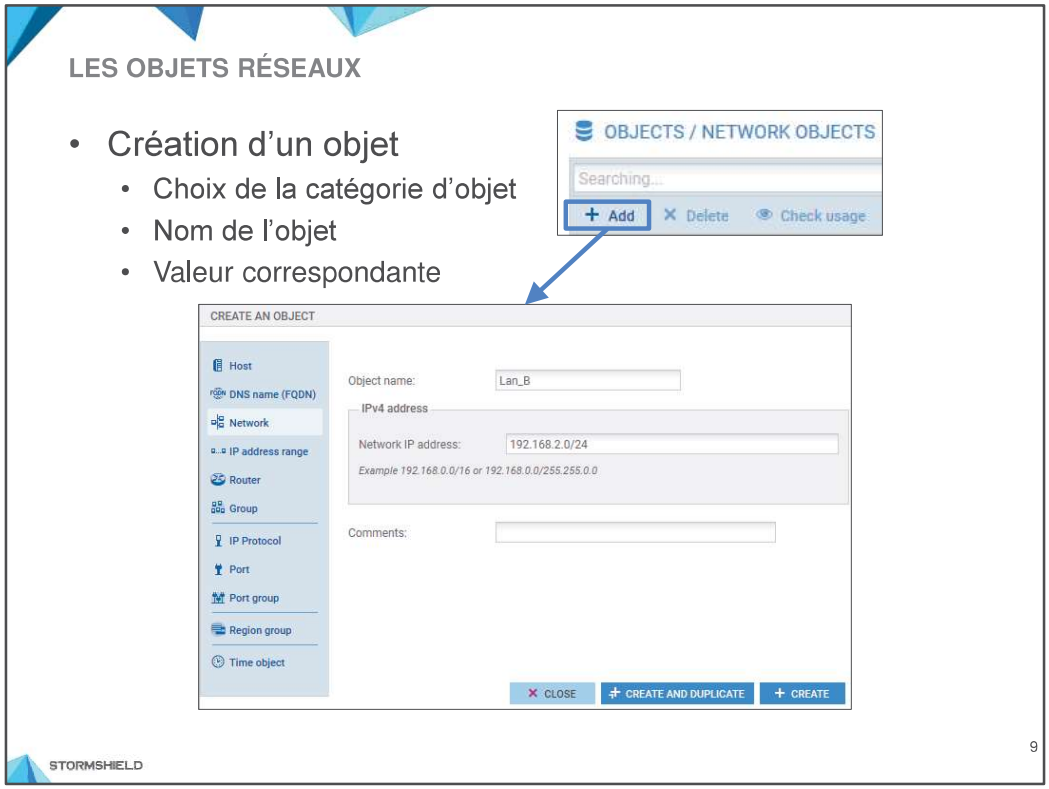


On peut distinguer deux catégories d'objets particuliers en plus des objets qui peuvent être créés par l'administrateur :

- **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 », créé automatiquement lorsqu'une adresse IP est associée à l'interface « OUT » ou l'objet « Network_internals » qui 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). Les figures ci-dessus représentent le protocole ICMP et l'objet « Internet ». Ce dernier regroupe l'ensemble des machines ne faisant pas partie des réseaux internes.

NOTE : Nous vous conseillons d'utiliser les objets implicites et préconfigurés et d'éviter de créer d'autres objets portant les mêmes valeurs.



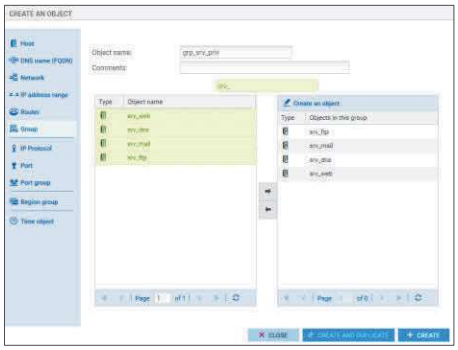
La fenêtre de création d'objets est composée de plusieurs onglets, un pour chaque catégorie.

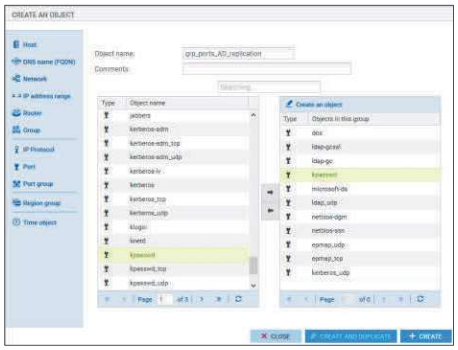
Dans la majorité des cas, la création d'un objet consiste à définir deux champs obligatoires, à savoir le nom et la valeur, le champ commentaire est facultatif.

Il est possible de « créer » ou de « créer et dupliquer » l'objet. Ce dernier bouton crée l'objet et maintient la fenêtre de création ouverte pour faciliter la création d'un nouvel objet de même catégorie.

LES OBJETS RÉSEAUX

- Création de groupes de machines ou groupes de ports
  - Nom de l'objet
  - Objets inclus dans le groupe

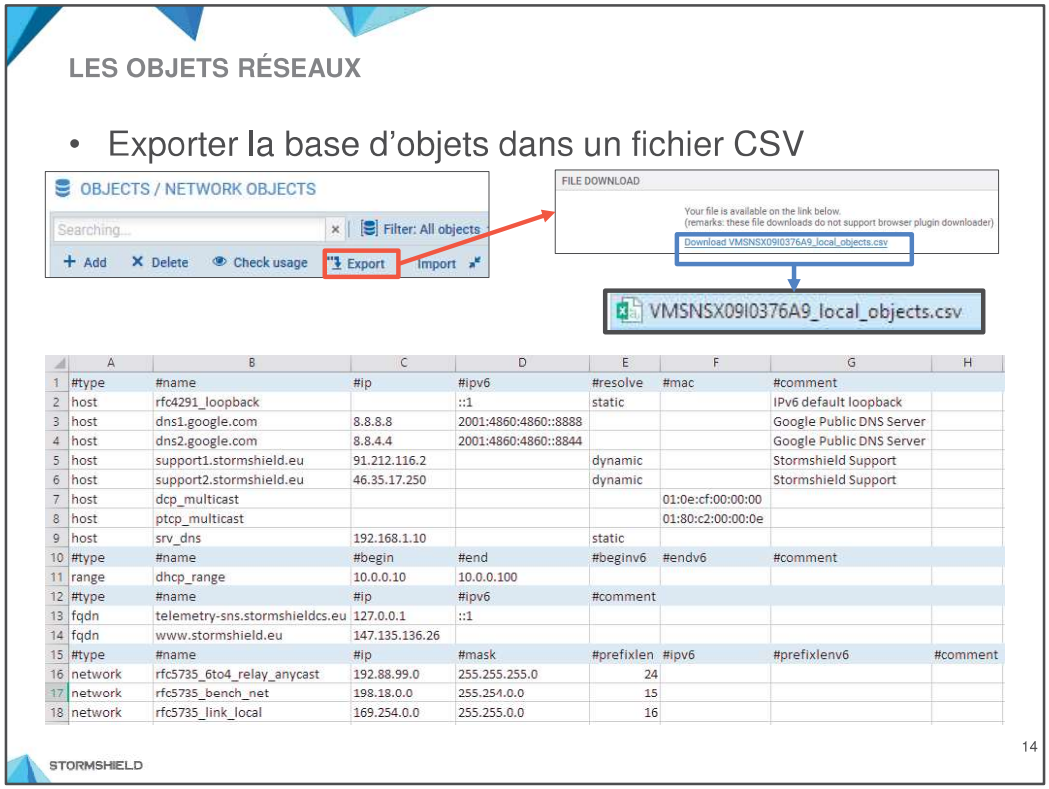




12

STORMSHIELD

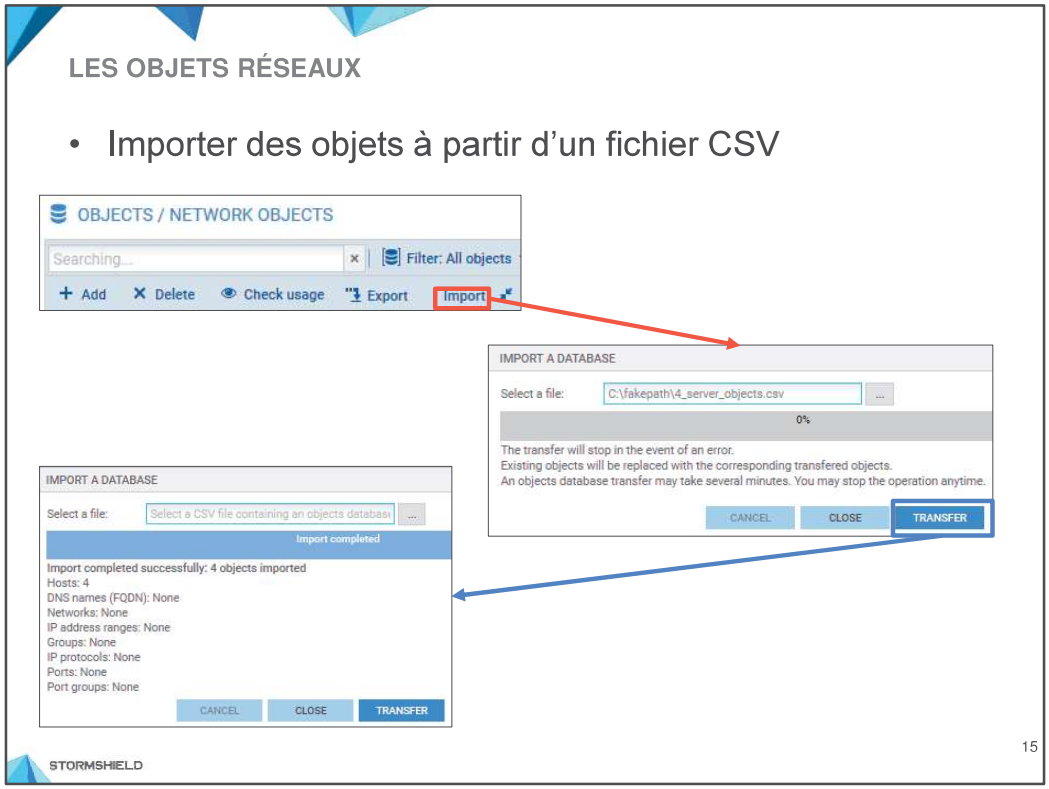
Pour ajouter un objet (ou plusieurs objets) au groupe, il suffit de sélectionner l'objet et de le basculer de la liste de gauche vers la liste de droite en cliquant sur le bouton →. La suppression de l'objet du groupe se fait par l'opération inverse avec le bouton ← .
Vous pouvez utiliser le champ de recherche sur une partie du nom ou de la valeur des objets souhaités.



	A	B	C	D	E	F	G	H
1	#type	#name	#ip	#ipv6	#resolve	#mac	#comment	
2	host	rfc4291_loopback		::1	static		IPv6 default loopback	
3	host	dns1.google.com	8.8.8.8	2001:4860:4860::8888			Google Public DNS Server	
4	host	dns2.google.com	8.8.4.4	2001:4860:4860::8844			Google Public DNS Server	
5	host	support1.stormshield.eu	91.212.116.2		dynamic		Stormshield Support	
6	host	support2.stormshield.eu	46.35.17.250		dynamic		Stormshield Support	
7	host	dcp_multicast				01:0e:cf:00:00:00		
8	host	ptcp_multicast				01:80:c2:00:00:0e		
9	host	srv_dns	192.168.1.10		static			
10	#type	#name	#begin	#end	#beginv6	#endv6	#comment	
11	range	dhcp_range	10.0.0.10	10.0.0.100				
12	#type	#name	#ip	#ipv6	#comment			
13	fqdn	telemetry-sns.stormshieldcs.eu	127.0.0.1	::1				
14	fqdn	www.stormshield.eu	147.135.136.26					
15	#type	#name	#ip	#mask	#prefixlen	#ipv6	#prefixlenv6	#comment
16	network	rfc5735_6to4_relay_anycast	192.88.99.0	255.255.255.0	24			
17	network	rfc5735_bench_net	198.18.0.0	255.254.0.0	15			
18	network	rfc5735_link_local	169.254.0.0	255.255.0.0	16			

Il est possible d'exporter la base d'objets dans un fichier CSV en cliquant sur le bouton « Exporter ». Le fichier sera proposé en téléchargement pour être stocké en local sur la machine. Le fichier CSV contient les objets machines, plages d'adresses IP, réseaux, FQDN, ports – plages de ports, protocoles, groupes et groupes de ports.

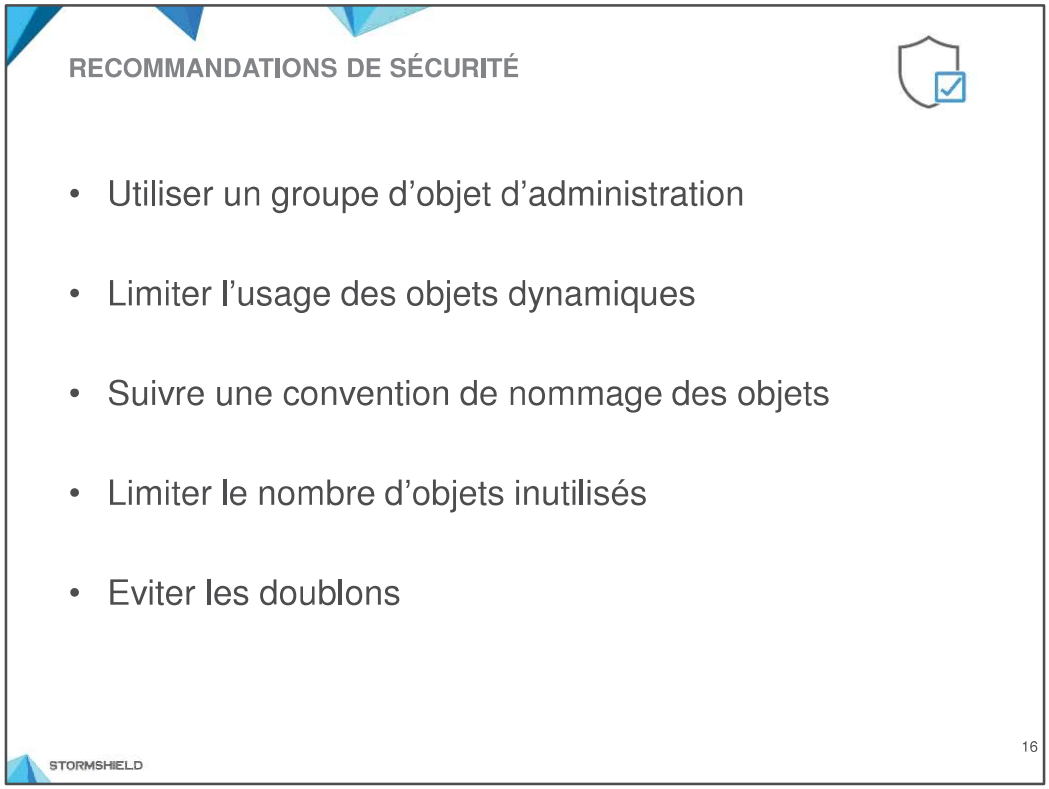
Les objets sont organisés par catégorie et séparés par des lignes contenant les noms des paramètres : #type, #name, #IP, etc… (les paramètres diffèrent en fonction des catégories d'objets). Les attributs d'un objet, quand à eux, sont séparés par des virgules.



Il est possible d'importer des objets depuis un fichier CSV possédant le même format que le fichier exporté.

Pour cela, il faut cliquer sur le bouton Importer, une fenêtre s'affiche pour permettre de renseigner le fichier CSV contenant les objets. Par la suite, il suffit de cliquer sur Transférer pour commencer l'import. Une barre d'avancement permet de visualiser le déroulement de l'import. Et une fois fini, un rapport statistique affiche le nombre d'objets importés par type.

NOTE : Les objets déjà existants sur le firewall sont remplacés par les objets transférés depuis le fichier.



Un groupe d'objet 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.

Les objets dynamiques (type FQDN et Dynamic Host) génèrent des requêtes DNS régulières. Cela sollicite le réseau et le pare-feu. Les objets enregistrés par défaut dans la configuration sont normalement inutiles si les recommandations précédentes on été mises en place (utilisation d'un miroir ou proxy interne).

Une convention de nommage bien définie et appliquée strictement évite la création de doublon et facilite la lecture des objets.

Les objets inutilisés chargent l'affichage et sont bien souvent oubliés et récréés. Afin d'éviter toute source potentielle de doublon, il est recommandé de ne pas conserver d'objets spécifiques inutilisés dans la configuration.

Les doublons doivent être traqués et supprimés, 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.