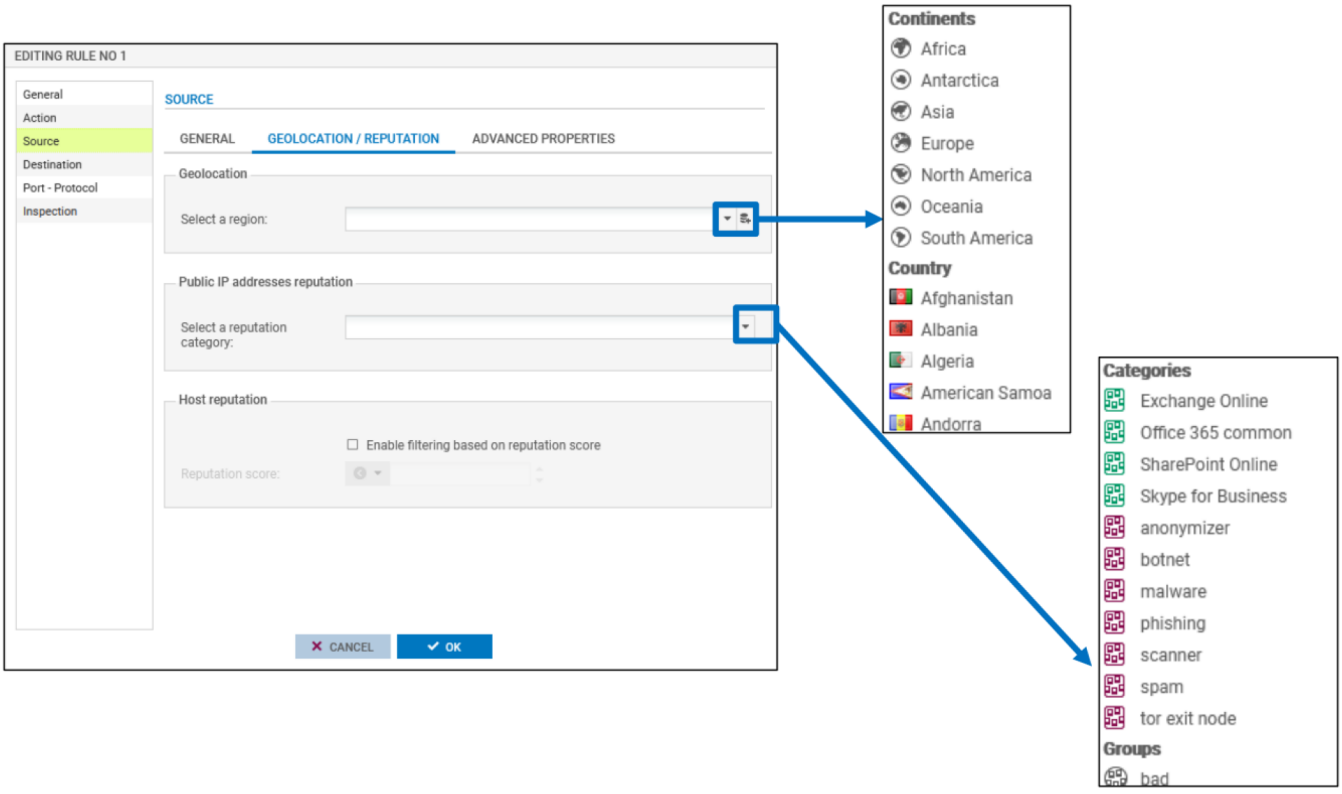
1. Activité : Fonctionnalités supplémentaires de filtrage

Dans une **règle** de filtrage, l'onglet **GÉOLOCALISATION / RÉPUTATION** du menu **Source** ou **Destination** permet d'ajouter un certain nombre de règles :

- **Géolocalisation** : permet de renseigner un continent ou un pays à l'origine du trafic. La liste ne contient pas d'adresses IP, le Firewall détermine le pays auquel appartient une IP, plutôt que de charger toutes les IP (les blocs d'adressage sont très fragmentés sur Internet).
- **Réputation des adresses IP publiques** : une IP publique peut avoir une réputation à la limite de deux catégories. Le groupe **Bad** créé dans le SNS Stormshield, regroupe les catégories : **anonymizer**, **botnet**, **malware**, **phishing**, **scanner**, **spam** et **tor**.
- **Réputation des machines** : Il est possible d'activer le filtrage selon le score de réputation des machines du réseau interne. Il faut au préalable activer la gestion de réputation des machines et définir les machines concernées par le calcul d'un score de réputation.



Dans le menu **Source** :

- les paramètres **Géolocalisation** et **Réputation des adresses IP publiques** sont utilisés généralement pour qualifier le **flux entrant** (provenant d'Internet),
- alors que le paramètre **Réputation des machines** est utilisé pour qualifier le flux sortant.

NOTE : Le score de réputation des machines internes, configurable dans ce menu, permet de préciser le **score** au-dessus duquel ou en-dessous duquel la règle de filtrage s'appliquera aux machines supervisées

Le group **bad** intègre toutes les catégories précédentes (de **anonymizer** à **tor exit node** - de **Anonymiseur** à **suspect**).

1.1. Retour

- Mise en oeuvre de l'UTM Stormshield

From:
https://siocours.lycees.nouvelle-aquitaine.pro/ - **Les cours du BTS SIO**

Permanent link:
https://siocours.lycees.nouvelle-aquitaine.pro/doku.php/activite4bfiltrage?rev=1699204751

Last update: **2023/11/05 17:19**