



Règle SNORT
(Blocage de l'extraction de données)

```
Block tcp $HOME_NET any -> 103.251.167.20 53 (msg:  
« trafic DNS vers IP malveillante »; sid: 10001; rev: 1;)
```

Bloque le trafic tcp sortant du réseau d'Echelon (« HOME_NET ») depuis n'importe quel port et en direction de l'adresse IP malveillante sur le port tcp 53.