

# STB v1 : Amélioration de la gestion des demandes en flux des utilisateurs

Juan PIRON

09 June 2017

## 1 Objet du document

Cette spécification définit les exigences relatives à une étude de la gestion en configuration des demandes de flux PGL via le logiciel CAPIRCA. Le besoin fonctionnel ayant été exprimés autour de 3 points :

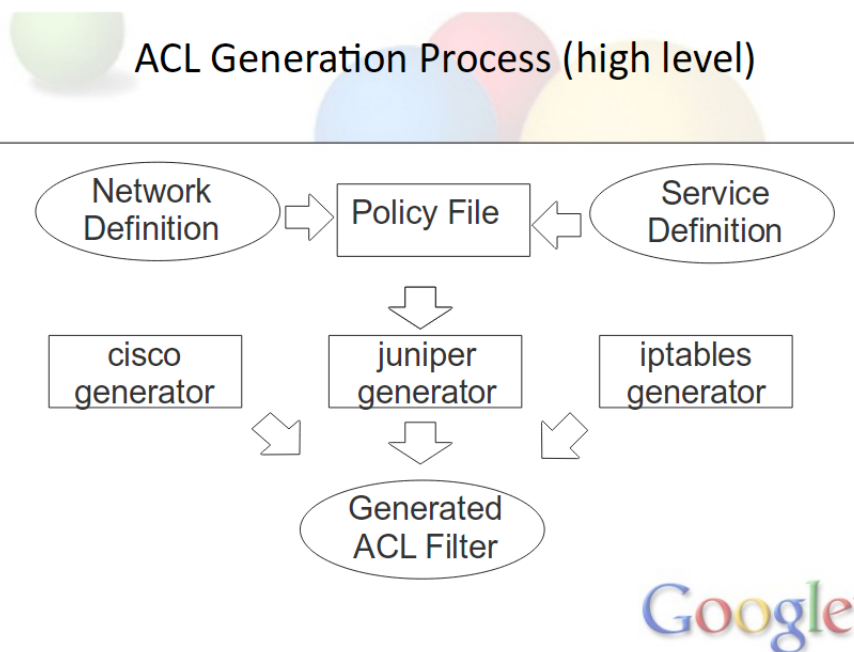
- 1/ adapter CAPIRCA pour la génération d'accès-liste ASA (similaires à celles des routeurs cisco).
- 2/ Mettre en place un mécanisme de génération des règles et de leur gestion en configuration à partir des demandes de flux utilisateurs.
- 3/ adapter les règles existant pour les injecter dans le système CAPIRCA.

## 2 Spécifications techniques actuelles

Le manager étant en mise à jour je n'ai pas pu voir de démonstration, cette section reste vide pour le moment. Des modifications risquent d'être apportées à la STB après visualisation de cette dernière.

## 3 Présentation générale de CAPIRCA

Capirca est un outil conçu pour utiliser des définitions communes des réseaux, des services et des fichiers de règles (politiques) de haut niveau pour faciliter le développement et la manipulation des listes de contrôle d'accès réseau (ACL) pour diverses plates-formes. Il a été développé par Google pour un usage interne et est désormais open source. Capirca simplifie le développement et la maintenance des filtres réseaux larges et complexes grâce à un seul et simple langage. Il fournit donc un langage de haut niveau facile à utiliser pour la définition des règles de sécurité réseau. Il permet la compilation des règles de sécurité en des filtres réseaux qui peuvent être appliqués à une variété de cibles (Cisco, Juniper, Iptables ...).



## 4 Spécifications techniques envisagées

### 4.1 Adapter Capirca pour la génération d'accès-list Cisco ASA

Capirca est constitué de plusieurs "generator", il y a du Cisco, de l'iptables etc. Après des apports de diverses sources Capirca n'a fait que s'enrichir avec le temps. Il faut savoir en effet que Capirca est disponible en open source sur git et toute contribution est la bienvenue. Il s'avère que l'une des dernières contributions est l'ajout du « generator » ciscoasa par Antonio Ceseracciu. Or ACLs des routeurs PGLs sont du type Cisco ASA v9.1. Cela répond au besoin. Néanmoins s'il existe des différences entre des versions d'ASA il suffira d'adapter le "generator" ciscoasa.

### 4.2 Mettre en place un mécanisme de génération des règles et de leur gestion en configuration à partir des demandes de flux utilisateurs

La solution envisagée ici est la création d'un "serveur" git, plus précisément Gobs. L'avantage de Gobs réside dans l'existence d'une interface web qui permettrait une gestion plus facile et intuitive des différentes ACLs. Tout cela bien sûr est en open source. Capirca sera placé sur un remote repository, il suffira simplement de créer la police ou de la modifier et de lancer le script

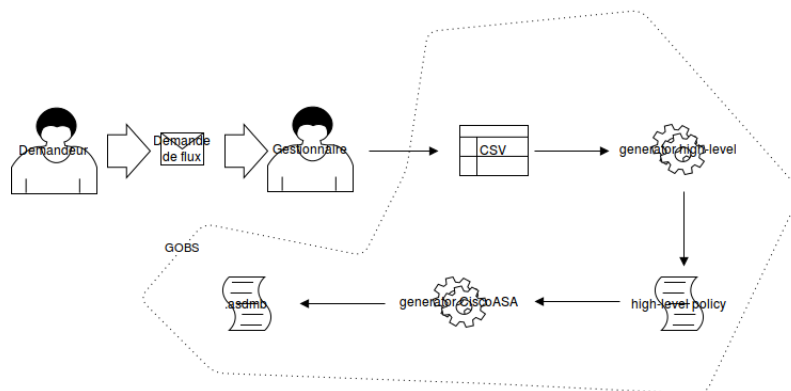
python, et par la suite de faire git add, commit et push. Les politiques (langage de haut niveau) seront présentes dans le répertoire capirca/policies/pol et les filtres (ACLs) dans le répertoire capirca/filters.

### 4.3 Adapter les règles existant pour les injecter dans le système CAPIRCA

En ce qui concerne les règles préexistantes sur les routeurs PGLs les injecter dans le système CAPIRCA revient à réécrire leurs politiques. Pour cela il serait possible de créer un script python ou Bash. Mais il s'avère que la manière brute d'écrire les différentes règles (répondant à une demande de flux utilisateur) se présente sous la forme d'un simple fichier CSV. Il paraît donc intéressant de créer un script qui produirait en sortie un fichier en langage de haut niveau. En d'autres termes créer le "generator" du langage de haut niveau de capirca.

Ou plus simplement injecter les ACLs existantes dans le répertoire filters sur Gobs. Et par la suite utiliser l'outil diff pour compiler les nouvelles aux anciennes.

Pour résumer l'une des solutions techniques proposées voire le schéma ci-dessous :



Par la suite, si le temps le permet, il pourrait être intéressant d'ajouter l'outil de "push" multi-plateform développé par Ryan Shea : LdPush. Cela faciliterait la mise à jour des différentes plateformes avec les nouvelles ACLs.