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

Juan PIRON

08 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 étaient exprimés autour de 3 points :

1/ Adapter CAPIRCA pour la génération d'accès-list 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.

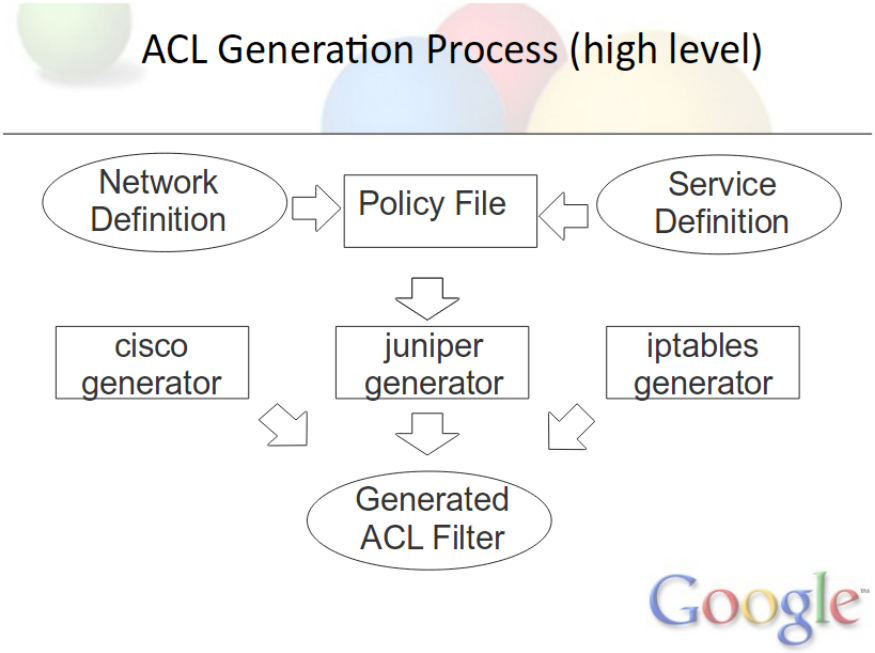
3/ Adapter les règles existante pour les injecter dans le système CAPIRCA.

2 Spécifications techniques actuelles

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 dévellopement 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 régles 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 et constitué de plusieurs "generator", il y'a du cisco, de l'iptables ... etc ... Après des aports de diverse source Capirca n'a fait que s'enrichir avec le temps. Il faut savoir en effet que Capirca et dipsoniple en open source sur git et toute contribution et la bien venue. Il s'avère que l'une des dernières contribution et l'ajout du « generator » ciscoasa par Antonio Ceseracciu. Or les accès listes des routeurs PGLs sont de type cisco ASA v9.1. Cela répond au besoin.

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 solutiuon envisagée ici est la création d'un "serveur" git, plus précisement Gobs. L'avantage de Gobs résidant dans l'existance d'une interface web qui permetrai une gestion plus facile et intuitive des différentes ACLs. Tout cela bien sur est en open source. Capirca sera placé sur un remote repository, il suffira simplement de creer la policie ou de la modifer et de lancer le script python, et par la siuite de faire git add, commit et push. Les policies (langage

de haut-niveau) seront présente dans le repertoire capirca/policies/pol et les filters (ACLs) dans le répertoire capirca/filters.

4.3 Adapter les règles existante pour les injecter dans le système CAPIRCA

En ce qui concerne les règles pré-existante sur les routeurs PGLs les injecters dans le système CAPIRCA revient à réécrire leur policies en d'autres termes à faire un reverse ingéniering. Pour cela il serait posible de créer un script python ou bash. Mais il s'avère que la manière brut d'écrire les différentes règles (répondant à une demmande de flux utilisateur) se présente sous la forme d'un simple fichier csv. Il paraît donc intéressant de créer un script qui produirai en sortie un fichier en langage de haut-niveau. En d'autres termes créé le generator du langage de haut niveau de capirca.

Pour résumer la solution technique proposé voir le shéma ci dessous :