

## Remerciements

Je tiens à remercier toutes les personnes qui ont contribué au succès de mon stage et qui m'ont aidé lors de la rédaction de ce rapport.

Ma gratitude s'adresse tout d'abord à mon professeur, **Mr Christian TOINARD**, tuteur de ce stage.

Je tiens à remercier vivement aussi mon maître de stage, **Mr Philippe CHARRON**, et le remercier pour son accueil et le partage de son expertise au quotidien. Grâce aussi à sa confiance, j'ai pu m'accomplir totalement dans mes missions. Il m'a été d'une aide précieuse dans les moments les plus délicats.

Je remercie encore toute l'équipe de Telespazio Guyane, dont j'ai pu apprécier l'esprit d'équipe et en particulier **Mr Christophe VIALON** et **Mr Julien MONEIN**, dont l'assistance m'a souvent été appréciable.

## Résumé

L'objectif de ce stage était l'étude de la possibilité de faire migrer les règles existantes d'un des firewalls principal (type **cisco ASA**) du **Centre Spatial Guyanais** (que l'on appellera **PGL**) dans le logiciel **google/capirca** et de mettre en place les mécanismes adéquats permettant la gestion de configuration des demandes de flux utilisateurs.

Cette demande s'articulait autour de 2 axes principaux. D'une part, la mise en place d'un mécanisme de génération des règles et leur gestion en configuration (git ou subversion ?) à partir des demandes de flux utilisateurs. D'autre part, l'adaptation des règles existantes pour les injecter dans le système **google/capirca**.

Capirca, développé par Google (d'où **google/capirca**), permet la génération d'access- lists de plusieurs types (cisco, junipers, iptables ...) et bien entendu **ciscoasa**, ce qui nous intéresse ici.

Au travers de différentes spécifications techniques, il a été proposé pour répondre à cette expression du besoin la mise en place d'un serveur git open source, **gogs** (go git service) embarquant **google/capirca** et d'une interface utilisateur de type shell/python pour la gestion des demandes de flux utilisateurs. L'interface prenait en compte la gestion des conflits qui peuvent exister entre le manager (**cisco ASDM – Adaptive Security Device Manager**), et les différents collaborateurs. En effet, les access-lists faisant partie des données ultrasensibles liées à l'activité spatiale, il est totalement interdit d'utiliser des serveurs tel que gitHub ou gitLab.

Pour des questions évidentes de sécurité et par précaution, une maquette a été mise en place pour la réalisation et la démonstration de ce projet. Cette maquette ressemble en tous points à la réalité, seules les adresses IPs sont fictives.

Le résultat de ce travail vise à permettre à tout gestionnaire présent dans le réseau du **PGL** de cloner le projet contenant l'interface de gestion et toutes les nouvelles demandes de flux. Il permet également d'en ajouter ou de modifier les existantes. Toujours à l'aide de l'interface, la nouvelle configuration peut ensuite être envoyée dans la running-config. Deux gestionnaires peuvent travailler sur les deux modes d'intégration existants (**google/capirca**, le **manager**), sans s'inquiéter des conflits pouvant être créés. Cette solution permet donc une réponse plus rapide mais aussi une gestion plus organisée des demandes de flux utilisateurs.

## Bibliographie

- <https://github.com/google/capirca/wiki>
- <https://gogs.io/docs>
- <http://www.cnes-csg.fr/web/CNES-CSG-fr/>
- <https://www.telespazio.fr/fr>
- <https://pynet.twb-tech.com/blog/automation/netmiko.html>

## Glossaire

- **ACL** : Une ACL est une liste d'Access Control Entry (ACE) ou entrée de contrôle d'accès donnant ou supprimant des droits d'accès à une personne ou un groupe.
- **ASDM** : Adaptive Security Device Manager, le manager.
- **Cisco ASA** : Depuis début 2005, Cisco a lancé une gamme de boîtiers (ASA 5510, 5520 et 5540) appelée Cisco ASA pour Adaptive Security Appliance.
- **CSG** : Centre spatial Guyanais
- **PGL** : Nom d'un firewall
- **REMUS** : réseau interne du CSG