Table des matières

[Introduction 2](#_Toc487678718)

[Telespazio Guyane et le Centre spatial guyanais 3](#_Toc487678719)

[Google/capirca une solution pour une gestion organisée des demandes de flux 3](#_Toc487678720)

[La gestion des demandes de flux utilisateurs 3](#_Toc487678721)

[Amélioration au travers de google/capirca 3](#_Toc487678722)

[REDEX (REtour D’EXperience) 3](#_Toc487678723)

[Conclusion 3](#_Toc487678724)

# Introduction

Ce stage de 4éme année d’école d’ingénieur, d’une durée de deux mois, a consisté à mettre en place CAPIRCA qui est un logiciel développé par GOOGLE pour automatiser la création des ACLs sur un firewall du centre spatial guyanais (CSG).

Ce rapport présente le travail que j’ai effectué lors de mon stage au sein de Telespazio Guyane, dans le centre technique du CSG. Il s’est déroulé du 6 Juin au 6 aout 2017.

Ce projet s’inscrivant dans la sécurité et se tenant au sein d’un lieu ultrasensible et demandant de multiple procédures sécuritaire, il s’est inscrit pleinement dans ma formation dont le cœur n’est autre que la sécurité des systèmes d’information.

Ce stage m’a permis d’entrevoir à quoi consiste le métier d’ingénieur dans ce secteur d’activité. Cela m’a aussi permis de mettre en œuvre d’ancien acquis de mon DUT tel que la manipulation de configuration de firewall.

Le but de ce résumé d’activité n’est pas de faire une description exhaustive de tous les aspects techniques mise en œuvre, mais de présenter de manière claire et synthétique les différentes parties techniques.

Dans un premier temps est présentée l’entreprise d’accueil, Telespazio France. Ensuite je vous présente les différents tâches de ce projet durant ces 2 mois. Pour finir, je reviendrai sur les apports de ce stage dans ma formation, et je conclurai.

# Telespazio Guyane et le Centre spatial guyanais

# Google/capirca une solution pour une gestion organisée des demandes de flux

## La gestion des demandes de flux utilisateurs

# description du réseaux REMUS demmandé demain comment cela ce passe.

Le firewall PRINC centralise les règles d’accès du centre technique, du CDL3 … de la base spatial. Il est configurer en deny all, c’est-à-dire que de base tous accès est rejeté. Toutes personnes, ou tous services désirant l’ouverture d’un accès, en fait la demande à la SI (Service Informatique). La SI transmet à Telespazio cette demande au travers d’une demande d’ouverture de flux utilisateur. Cette demande ce présente sous la forme d’un fichier constitué : d’une référence, du nom et prénoms du demandeur … mais surtout des différents accès à ouvrir. Etant indiqué les adresses ips, les ports, les services et le sujet de cette ouverture.

Une fois cette demande reçu par Telespazio elle est transmise à une personne que l’on nommera, dans le cadre de ce résumé d’activité, gestionnaire. Ce gestionnaire se chargera alors d’ouvrir les différents accès en ajoute les ACLs correspondantes dans le firewall PRINC.

Pour réaliser cela le gestionnaire doit ce placer au niveau du réseau privé du PRINC et se connecter au manager. Le manager n’est autre que le ciscoa asdm, en effet le PRINC et un firewall de type ciscoasa.

# gestion par interface ici ou après

Cette manipulation prend du temps, notamment car elle ne peut être réalisé de n’importe où, elle demande en effet d’être physiquement présent derrière une machine précise qu’est le manager. Mais aussi parce que l’ajout des règles au niveau du manager est long et fastidieux, surtout quand on sait qu’une demande d’ouverture de flux demande en moyenne l’ajout d’une dizaine d’ACLs.

Le manager permet l’ajout d’ACLs mais aussi d’objets. Un objet peut être l’ip d’un hôte, d’un réseau, un service (par exemple : https), une liste de protocole … ces objets correspondent bien entendus à des objets de type ciscoasa. Ils apparaissent donc dans la running config.

Or il n’est pa toujours créé d’objet pour chaque ip, ainsi souvent on ce retrouve avec des doublons au sein du PRINC, ce qu’il faut le dire ne pose pas de problème en termes de fonctionnement. Prenons un exemple simple : le gestionnaire A traite une demmande de flux à l’aide d’objets créé ou près existants. Le gestionnaire B fait de même avec une autre demmande d’ouverture de flux. Il s’avère qu’entre ces deux demmande 4 règles était similaire. Etant donné que leur méthode d’ajout et différente et qu’il n’y a aucun système de détection, il y a doublon.

Il faut ajouter concernant la technique de gestion actuelle au travers du manager, que cette dernière ne permet pas de garder un visuel sur les demandes de flux traitées. En d’autres, termes on ne peut pratiquement pas retrouver une demande de flux dans la configuration du PRINC avec ou sans le manager, après traitement de cette dernière.

Sinon outre tous ses aspects positifs tels qu’une visualisation amélioré des ACLs, sans le manager ( en oubliant la cli) il n’y plus de moyens « facilité » de configuration du PRINC.

C’est dans ce cardre que l’on introduire google/capirca.

## Google/capirca

## Google/capirca appliqué au PRINC

# REDEX (REtour D’EXperience)

# Conclusion