NetFlow et ALCASAR

Analyse de flux IP avec le protocole NetFLow

Emmanuel BAUDVIN
Lucien CASSAGNES
Antoine PUISSANT

Enseignant : M. REY

2014 - 2015

Résumé

ALCASAR est un projet libre de contrôle d'accès au réseau, un NAC. Au sein de ce dernier, il est possible de retrouver l'utilisation du protocole NetFlow. ALCASAR bénéficie alors d'une sonde réseau lui permettant d'analyser les flux réseaux le traversant avec beaucoup de finesse.
Durant ce projet, le but est d'assimiler le fonctionnement du protocole NetFlow seul et au sein d'ALCASAR.
Une fois cet apprentissage fait, nous devrons comparer la version de NetFlow présente dans ALCASAR à la dernière version. Cette comparaison devra permettre de savoir s'il est utile de faire évoluer la version d'ALCASAR. En cas de résultats positifs, la mise à jour devra être réalisée et testée.

Table des matières

1 Introduction

1.1 Le projet ALCASAR

Le projet ALCASAR est né suite à une demande d'une entité gouvernementale voulant assurer la traçabilité et l'imputabilité des connexions de tous les utilisateurs connectés à leur réseau.
Après une rapide étude de marché, les responsables de projet se sont rendu compte qu'il n'existait pas de solution libre de droits permettant de remplir les demandes précises de l'entité : intercepter, authentifier, filtrer et imputer l'accès aux utilisateurs à internet.
Ainsi, les chefs du projet ont alors décidé de réaliser eux-mêmes un contrôleur d'accès pouvant répondre aux besoins du projet. C'est ainsi que le projet ALCASAR à vu le jour.

FIGURE 1: Logo d'ALCASAR

Afin de pouvoir réaliser ces fonctions d'interception ou de filtrage, ALCASAR va embarquer plusieurs outils d'analyse de flux. Parmi ces outils, nous allons pouvoir retrouver NetFlow.

1.2 NetFlow

NetFlow est un protocole qui a été conçu par Cisco Systems. Il va permettre de réaliser une surveillance des réseaux en collectant des informations sur les flux IP. Ce produit va permettre à un administrateur réseau de déterminer différentes informations telles que la source et la destination du trafic, le type de service utilisé ou encore la cause de nœuds de congestion.

1.3 IPFIX

A voir : `http://www.bradreese.com/blog/netflow-vs-ipfix-exporter.htm`

2 Partie 2

2.1 Sous-titre 2

Références

[1] ALCASAR. *Projet ALCASAR*. 2015. URL : http://www.alcasar.net/.

[2] AUTHOR. *REF TITLE*. ORG. 2015. URL : http://www.url.com/.