CONCEPTION ET DEPLOIEMENT D'UNE ARCHITECTURE RESEAU SECURISEE

TEDJANI Mebarka & AMMARI Fattoum
Département d'informatique et de technologies d'information
Université Kasdi Merbah Ouargla 30000, Algérie
ammari.fattoumrcs@gmail.com & mebarkatidjani@gmail.com

Résumé

Au cours de ces dernières années, l'utilisation du protocole Internet (Internet Protocol, IP) comme base des réseaux téléinformatiques est devenue très importante, que ce soit par l'utilisation croissante de l'Internet ou dans le cadre de réseaux d'entreprises de type intranet. Si la flexibilité d'IP et sa simplicité ont su répondre aux besoins en matière de réseaux informatiques de ces dernières décennies, le but de ce protocole n'a jamais été d'assurer des communications sécurisées, d'où l'absence de fonctionnalités dans ce domaine. La facilité des attaques, le fait que la démocratisation de l'Internet les rende accessibles à beaucoup et la volonté croissante de pouvoir utiliser des réseaux IP pour des applications sensibles ont donc poussé au développement de diverses solutions de sécurité : gardes-barrières, routeurs filtrants, protocoles et applications sécurisées se sont multipliés, [1-2].

Les ACL (en anglais « Acces Control Lists ») ou en Français « Listes de Contrôle d'Accès », nous permettent d'établir des règles de filtrage sur les routeurs, pour régler le trafic des datagrammes en transit.

Mots clés : ACL, Filtrage, Sécurité réseau, contrôle d'accès.

1. Introduction

Le réseau est un point sensible du système : du fait de sa connexion vers le monde entier il offre à des individus physiquement éloignés, comme aux employés, un accès à vos données. Quel que soit sa taille, le réseau subit des risques. Il est important de signaler qu'on ne peut pas maintenir la totalité d'un parc sans trou de sécurité, [3].
La sécurité est avant tout un ensemble de préconisations qu'il faut adapter aux besoins de chaque cas rencontré. Il n'y a pas une seule méthode mais un ensemble de notions à prendre en compte.
La sécurité à mettre en œuvre dépend principalement des moyens qui seront mis en œuvre pour les attaques et donc principalement de ce qui est à sécuriser. Il s'agit de trouver un juste équilibre entre le coût de la sécurité et les risques à assumer.
Il est essentiel de connaître les ressources de l'entreprise à protéger (Dans notre cas la SONELGAZ-GRTE) et de maîtriser le contrôle d'accès et les droits des utilisateurs du système d'information, [4].

2. Préliminaires

Les ACL permettent de mettre en place un filtrage dit « statique » des datagrammes, c'est-à-dire d'instaurer un certain nombre de règles à appliquer (fig. 1) sur les champs concernés des en-têtes des divers protocoles.

Une ACL est une liste de règles. Chaque règle est du type (condition, action). Les règles sont interprétées *séquentiellement*. Si la condition analysée ne correspond pas, on passe à la règle suivante. Si la condition correspond, l'action correspondante est effectuée, et le *parcours de l'ACL est interrompu. Par défaut, toutes les ACL considèrent la règle (VRAI, REJET)* si aucune des règles précédentes n'a été prise en compte, c'est-à-dire que ***tout datagramme non explicitement accepté par une règle préalable sera rejeté.***

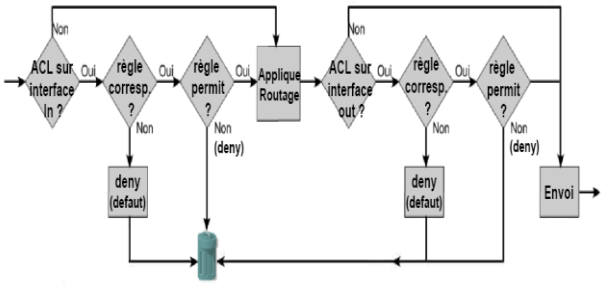

Fig 1. Principe des ACLs

3. Résultats

La figure suivante représente l'architecture du réseau SONELGAZ-GRTE crée à l'aide du l'émulateur GNS3.

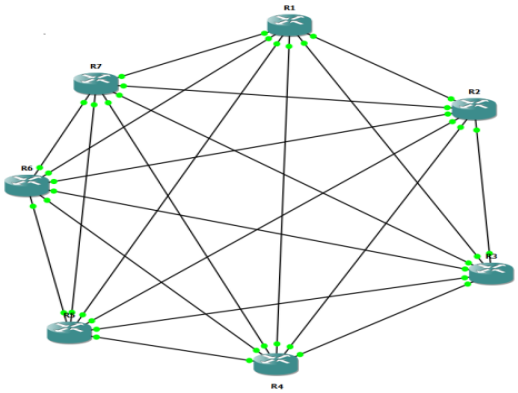

Fig 2. Architecture du réseau SONELGAZ-GRTE (GNS3).

Filtrage des paquets : configuration des ACLs sur un routeur; Création de liste d'accès pour limiter au VTY

```
Router>
Router > ena
Router # config t
Router (config) # line vty 0 4
Router (config-line) # password mot_de_passe
Router (config-line) # login
```

4. Références

[1] R. Legrand et A. Vaucamps, "CISCO-Notiond de base sur les réseaux," Eni, 2014, 1er module examen CCNA.
[2] G. Avoine, P. Junod et P. Oechslin, "Sécurité informatique,"*Vuibert 2e Edition*, 2010,286 p.
[3] M. Zalewski, "Menaces sur les réseaux," *Pearson Education 1e Edition*, Janvier 2009, 320 p.
[4] C. Pernet, "*Sécurité et espionnage informatique*,"Eyrolles, 2014, 240 p.