Cahier des charges: Unified Threat Management

Guillaume ROUVIÈRE, Mohammed DJOUDI,
Frédéric BORDI, Cédric LESEC

5 février 2009

Table des matières

Table des figures

0.1 Présentation : Unified Threat Management

0.1.1 Qu'est ce qu'un UTM ?

Un UTM (comprendre Unified Threat Management ou Gestion Unifiée des Menaces) est destiné comme son nom l'indique à sécuriser un accès réseau sur tous les axes. C'est à dire gérer les divers problèmes de sécurité comme les intrusions, les virus, les spams, etc. ... Il réalise la plupart du temps un pont entre un réseau à sécuriser et un réseau non-sécurisé en utilisant un pare-feu, un antivirus, et bien d'autres modules décrits plus loin.

0.1.2 Utilisation de l'UTM

Notre UTM sera destiné à protéger un réseau privé des menaces d'Internet. Il devra s'utiliser de façon transparente, c'est à dire sans nécessiter de configuration poussée de la part des hotes du réseau privé. Nous allons privilégier la conception du réseau privé en WIFI. Ainsi ce boitier se placera entre le modem (box telle que livebox, freebox, neufbox, etc. ...) et les ordinateurs hotes et ces derniers se connecterons au réseau en WIFI.

0.1.3 Pourquoi ce choix ?

Nous avons choisi ce sujet, car nous souhaitons tous les quatres faire du réseau, de son administration et de sa sécurité un objectif de profession. Travailler sur les UTM, qui sont la nouvelle tendance en matière de sécurité réseau, nous permettra d'apréhender plus facilement les problèmes de notre futur métier. De nombreux UTM existent, mais les versions libres et gratuites sont moins présentes. Le but de ce TER sera pour nous, de nous approprier les divers outils des UTM en concevant le notre, et d'essayer d'innover en apportant d'autres fonctionnalités lorsque celle de base seront opérationnelles.

0.2 Cahier Des Charges

0.2.1 Fonctionnalités à inclure

La première fonctionnalité indispensable à inclure est celle du pare-feu. En effet, pour protéger efficacement le sous réseau un pare-feu efficace doit être configuré. Pour cela nous allons utiliser IPTables, l'interface en ligne de commande du pare-feu de linux : NETFILTER. Grâce à cela, nous allons pouvoir définir une zone "démilitarisée", plus communément connue sous le nom de DMZ. Cette zone est telle que seul les paquets potentiellement autorisés seront succeptible de pénétrer. Ensuite, dans cette DMZ nous allons implanter des fonctionnalité de serveur mandataire, d'anti-virus, d'anti-spam, ainsi qu'un IPS (Intrusion Prevention System), ce dernier étant destiné à analyser les flux de données transitant par le routeur et à couper la connexion si une menace se fait sentir. Un annuaire LDAP sera aussi déployé, afin de gérer les identifiants de connexions. Il y aura de plus un serveur web apache pour modifier et paramétrer le tout, ainsi qu'un serveur ssh pour accéder à l'ordinateur. Voici un schéma de ce projet :

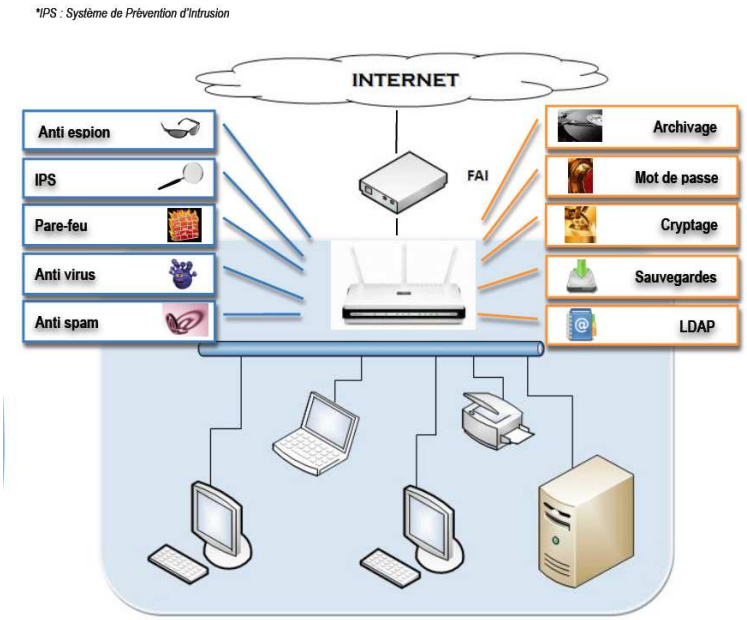

Fig. 1 – Représentation de l'UTM

Donc en récapitulant, on obtient :

- Configuration/Installation du matériel, et des serveurs DHCP, DNS, Apache, et SSH pour faciliter la connexion et le travail sur la machine même et à distance
- Configuration/Installation du Pare-Feu et définition des politiques de sécurité
- Configuration/Installation du ou des serveur mandataires
- Configuration/Installation des Anti-virus
- Configuration/Installation de l'IPS
- Configuration/Installation de l'Anti-Spam
- Configuration/Installation d'un annuaire LDAP
- Création de l'interface web
- Création de notre distribution Linux
- Configuration/Installation des autres fonctionnalités facultatives

Le choix de notre distribution linux de base est Debian, car les mises à jour peuvent être automatisées et c'est un système que nous connaissons bien.

0.3 Objectifs

0.3.1 Répartition

Ensembles Des Taches

Voici le diagramme de Gantt qui donne un aperçu des étapes du projet.

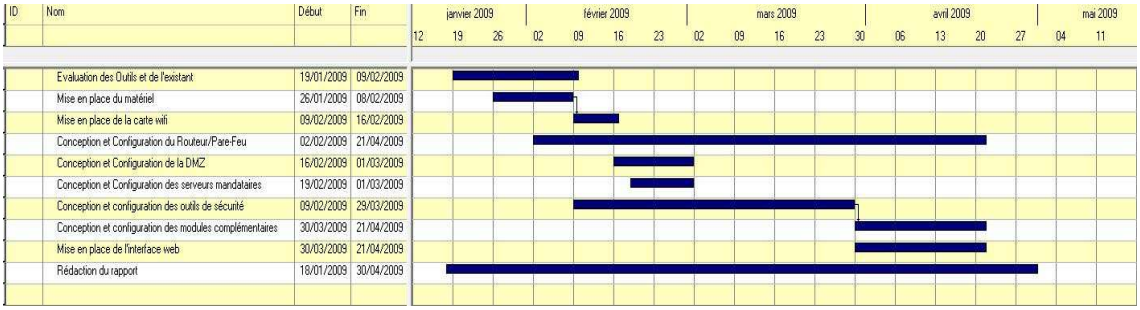

Fig. 2 – Diagramme de Gantt

La répartition des tâches n'est pas fixée entre les membres de l'équipe. En effet, chacun se voit attribué une nouvelle tâche à effectuer, lorsqu'il a fini la précédente. Le but étant d'insérer le plus de modules possible. Un fort travail en équipe est de toute manière nécessaire car en sécurité informatique plusieurs regards valent mieux qu'un.

Réunions

Nous avons décidé pour le moment de nous réunir les lundi, mercredi et vendredi de chaques semaines. Nous utilisons ces réunions pour travailler ensemble aussi et mettre en commun le travail réalisé. Un compte-rendu sera effectué par semaine.

0.3.2 Objectifs Primaires

L'objectif primaire est de concevoir notre distribution de linux intégrant les fonctionnalités de base retrouvées sur n'importe quel UTM du marché, avec une interface web pour la paramétrer. Bien entendu, la principale difficulté est d'apprendre comment tout coordonner, tout correctement paramétrer et répondre aux besoins de sécurité. Ces fonctionnalités sont détaillées à la section cahier des charges.

0.3.3 Objectifs Secondaires

Notre objectif secondaire sera d'ajouter des fonctionnalités supplémentaires facultatives telles que des serveur de fichiers, et l'encryptage de fichiers. En effet, il serait utile que cet UTM dérive son utilité en ne s'occupant plus seulement des aspects sécurité à proprement parlé. Ces objectifs seront abordés si nous en avons le temps.

0.3.4 Premières Difficultés

Les premières difficultés que nous rencontrons déjà sont dues au matériel, notamment les cartes wifi. Ces dernières doivent, en plus d'être compatibles linux, être paramètrable en point d'accès. Cet aspect devrait être résolu rapidemment.