

## ملخص

جدار الحماية هو أداة ضرورية وفعالة في مجال المعلوماتية. لكن مع مشكلة تشفير المعلومات أصبحت الحماية غير كاملة. في هذه المذكرة قمنا بانجاز أداة تسمح بمعالجة و تفتيش المعلومات المشفرة بين زبون و سيرفير بتطبيق تقنية رجل الوسط الموثوق مع عمل تغييرات على رسائل المصافحة. هذه الأداة تعمل اتصال مزدوج مع الزبون و السيرفير في نفس الوقت من اجل الحصول على مفاتيح التشفير. بعد هذه العمليات تستطيع الأداة قراءة المعلومات المشفرة.

**كلمات مفتاحية :** جدار الحماية, رجل الوسط, رجل الوسط الموثوق.

## Abstract

The firewalls are necessary tools in computing security domain, but with the problem of encrypted traffic make its functionalities imperfect.

So, in this these we are implementing a tools allow to analyze and inspect the SSL encrypted traffic between client and server with **Trusted Man in The Middle** technique with modification of handshake messages. Our module firewall communicate with the two partners and play the role of client and server in the same time then exchanging them publics keys in order to take session key. After all this operations our module can read all the traffic.

**Key words:** firewall, SSL traffic, Man in The Middle, Trusted Man In The Middle.

## Résumé

Les pare-feux sont des outils plus importants dans le domaine de sécurité informatique. Mais avec le problème de trafic crypté son fonctionnement sera incomplet. Donc dans ce mémoire on a implémenté un outil permet d'analyser et inspecter le trafic chiffré SSL entre un client et un serveur à l'aide d'une technique **Trusted Man In The Middle** avec la modification des messages **Handshake**. Notre module pare-feu communique avec les deux partenaires en jouant le rôle d'un client et d'un serveur au même temps et faire échanger leurs clés publiques, afin d'obtenir la clé de session. Après ces opérations le module peut déchiffrer tout le trafic passe par lui.

**Mots clé:** pare-feu, trafic SSL, Man In The Middle, Trusted Man In The Middle.

---