

Table des matières

Chapitre I - Les pare-feux

Introduction générale.....	6
1.1 Introduction	6
1.2 Qu'est-ce qu'un pare-feu?	6
1.3 Fonctionnement d'un système pare-feu	7
1.4 Les catégories des pare-feux	8
1.4.1 Le filtrage simple de paquets	8
1.4.2 Le filtrage dynamique.....	9
1.4.3 Le filtrage applicatif	10
1.5 Le pare-feu et le problème de trafic crypté	11
1.6 Conclusion :	11

Chapitre II - Le protocole SSL(Secure Socket Layer)

Le protocole SSL(Secure Socket Layer).....	12
2.1 Introduction	13
2.2 Origine.....	13
2.3 Cas d'utilisation.....	14
2.4 Fonctionnalités	15
2.5 Composition	16
2.5.1 Le protocole SSL handshake :	17
2.5.2 Le protocole SSL Alert.....	21
2.5.3 Le protocole SSL Record	21
2.6 Tunnel HTTPS	25
2.7 Limitations	26

2.8 Infrastructure à clés publiques	26
2.8.1 Composition.....	27
2.8.2 Les certificats numériques	27
2.8.3 Le certificat X.509	29
2.9 Conclusion.....	31

Chapitre III - Inspection du trafic SSL

Inspection du trafic SSL	30
3.1 Introduction.....	33
3.2 L'attaque Man In The Middle.....	33
3.2.1. Les techniques d'attaque Man in the Middle.....	34
3.2.2. Les outils d'attaque MITM.....	35
3.3. Sniffer trusted man in the middle (Sniffer TMITM).....	37
3.3.1 Homme de milieu confiant avec deux sessions SSL/TLS séparées	37
3.3.2 Homme au milieu confiant avec la modification de Handshake	39
3.4 Conclusion.....	43

Chapitre IV - Implémentation et réalisation

4.Introduction	45
4.2Application	45
4.2.2 Cryptage de données.....	46
4.2.3 Les Commandes de Java Keytool pour la Création et l'Import	46
4.3 Implémentation.....	47
4.4 Démonstration	48
4.5 Conclusion.....	48
Conclusion générale	49

