

République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

CEntre de Recherche sur l'Information Scientifique et Technique



*Mémoire pour l'obtention du diplôme de  
Post graduation spécialisée en sécurité informatique*

Thème

**Déploiement d'une politique de sécurité  
à base d'IPSec  
pour la CNEP-BANQUE**

**Présenté par :**

*Mr DAACHI Abdelaziz  
Mr SOLTANI Zohir*

**Encadré par :**

*Dr. TANDJAOUI Djamel*

**Membres du jury**

- Pr BADACHE Nadjib   Président*
- Mr MEZIANE Abdelkrim   Examineur*
- Mr BOUDINA Abdelmadid   Examineur*

CERIST 2006

<b>INTRODUCTION.....</b>	<b>4</b>
<b>CHAPITRE 1 : LES RESEAUX INFORMATIQUES</b>	
<b>1.1 GENERALITES.....</b>	<b>7</b>
<b>1.2 CLASSIFICATION DES RESEAUX SELON LA TAILLE.....</b>	<b>7</b>
<b>1.3 CLASSIFICATION DES RESEAUX SELON LA TOPOLOGIE .....</b>	<b>8</b>
<b>1.4 LE MODEL DE REFERENCE OSI DE L'ISO .....</b>	<b>9</b>
1.4.1 LA COUCHE PHYSIQUE.....	10
1.4.2 LA COUCHE LIAISON.....	10
1.4.3 LA COUCHE RESEAU .....	10
1.4.4 LA COUCHE TRANSPORT .....	11
1.4.5 LA COUCHE SESSION .....	11
1.4.6 LA COUCHE PRESENTATION .....	11
1.4.7 LA COUCHE APPLICATIONS.....	11
<b>1.5 RESEAU INTERNET ET LE PROTOCOLE TCP/IP.....</b>	<b>11</b>
1.5.1 HISTORIQUE ET ORGANISATION D'INTERNET .....	11
1.5.2 ARCHITECTURE DES PROTOCOLES TCP/IP .....	12
<b>1.6 COMPARAISON ENTRE LE MODELE OSI ET TCP/IP .....</b>	<b>14</b>
<b>1.7 ADRESSAGE .....</b>	<b>14</b>
<b>1.8 NOMMAGE .....</b>	<b>15</b>
<b>1.9 RESEAU ETHERNET .....</b>	<b>15</b>
<b>1.10 LIAISON SLIP.....</b>	<b>16</b>
<b>1.11 LA LIAISON PPP.....</b>	<b>16</b>
<b>1.12 PROTOCOLES ARP ET RARP .....</b>	<b>17</b>
<b>1.13 PROTOCOLE IP .....</b>	<b>17</b>
<b>1.14 DATAGRAMME IP .....</b>	<b>18</b>
<b>1.15 LE ROUTAGE.....</b>	<b>20</b>
<b>1.16 PROTOCOLES TCP ET UDP .....</b>	<b>22</b>
<b>1.17 LES APPLICATIONS.....</b>	<b>23</b>
<b>1.18 CONNEXION A DISTANCE (TELNET).....</b>	<b>23</b>
<b>1.19 TRANSFERT DE FICHER (FTP).....</b>	<b>23</b>
<b>1.20 COURRIER ELECTRONIQUE (SMTP).....</b>	<b>23</b>
<b>1.21 CONCLUSION.....</b>	<b>23</b>
<b>CHAPITRE 2 : LES PROTOCOLES DE SECURITE</b>	
<b>2.1 DEFINITION D'UN PROTOCOLE .....</b>	<b>24</b>
<b>2.2 PROTOCOLES ORIENTES CONNEXION.....</b>	<b>24</b>
<b>2.3 PROTOCOLES NON ORIENTES CONNEXION.....</b>	<b>24</b>
<b>2.4 SERVICES ET MECANISMES DE SECURITE .....</b>	<b>28</b>
2.4.1 SERVICES DE SECURITE : .....	28
2.4.2 MECANISMES DE SECURITE .....	29
<b>2.5 PROTOCOLES DE SECURITE .....</b>	<b>30</b>
2.5.1 PROTOCOLE NTLM.....	30
2.5.2 PROTOCOLE SSL.....	31
2.5.3 PROTOCOLE SSH.....	33

<b>2.6 INTERNET PROTOCOL VERSION 6 (IPV6)</b> .....	<b>33</b>
<b>2.7 FONCTIONNALITES IPV6</b> .....	<b>34</b>
<b>2.8 PAQUET IPV6 SUR SUPPORT DE RESEAU LOCAL</b> .....	<b>35</b>
<b>2.9 FORMAT DU DATAGRAMME IPV6</b> .....	<b>35</b>
<b>2.10 SYNTAXE DES ADRESSES IPV6</b> .....	<b>37</b>
<b>2.11 UTILISATION D'UNE ADRESSE IPV6 COMME NOM D'HOTE</b> .....	<b>37</b>
<b>2.12 NOTATION DES MASQUES DE SOUS RESEAU</b> .....	<b>38</b>
<b>2.13 QUELQUES DIFFERENCES ENTRE IPV4 ET IPV6</b> .....	<b>38</b>
<b>2.14 CONCLUSION</b> .....	<b>38</b>

### **CHAPITRE 3 : LE PROTOCOLE IPSec**

<b>3.1 DEFINITION</b> .....	<b>40</b>
<b>3.2 SERVICES DE SECURITE FOURNIS PAR IPSEC</b> .....	<b>40</b>
3.2.1 CONFIDENTIALITE DES DONNEES .....	41
3.2.2 AUTHENTIFICATION .....	41
3.2.3 INTEGRITE .....	41
3.2.4 PROTECTION CONTRE LE REJEU .....	42
<b>3.3 ARCHITECTURE D'IPSEC</b> .....	<b>42</b>
3.3.1 AUTHENTICATION HEADER (AH) .....	42
3.3.2 ENCAPSULATING SECURITY PAYLOAD (ESP) .....	45
<b>3.4 GESTION DES CLÉS</b> .....	<b>47</b>
3.4.1 TYPES DE CLES .....	48
3.4.2 INFRASTRUCTURES A CLES PUBLIQUES .....	48
3.4.3 GESTION DES ASSOCIATIONS DE SECURITE ET DES CLES .....	48
3.4.4 PHASE1 ETABLIR UN CANAL SECURISE.....	50
3.4.5 PHASE 2 NEGOCIATION DES ASSOCIATIONS DE SECURITE .....	52
<b>3.5 LES ASSOCIATIONS DE SECURITE (SA)</b> .....	<b>53</b>
<b>3.6 POLITIQUES DE SECURITE</b> .....	<b>54</b>
3.6.1 PRINCIPE DE FONCTIONNEMENT .....	55
<b>3.7 CONCLUSION</b> .....	<b>56</b>

### **CHAPITRE 4 : CONCEPTION DE LA SOLUTION**

<b>4.1 ETUDE DE L'EXISTANT</b> .....	<b>59</b>
<b>4.2 ORGANIGRAMME HIERARCHIQUE DE LA CNEP</b> .....	<b>60</b>
<b>4.3 PRESENTATION DU SYSTEME D'INFORMATION</b> .....	<b>62</b>
<b>4.4 CLASSIFICATION DES SYSTEMES INFORMATIONNELS</b> .....	<b>62</b>
<b>4.5 RESEAU PUBLIC EN ALGERIE</b> .....	<b>64</b>
4.5.1 VSAT.....	65
4.5.2 DZPAC.....	65
4.5.3 INMARSAT .....	65
4.5.4 GMPCS .....	65
4.5.5 CERIST .....	66
<b>4.6 SOLUTION PROPOSEE</b> .....	<b>67</b>
<b>4.7 CONCLUSION</b> .....	<b>72</b>

**CHAPITRE 5 : DEPLOIEMENT DE LA SOLUTION**

<b>5.1 DEPLOIEMENT D'IPSEC AVEC WINDOWS 2000 SERVEUR .....</b>	<b>73</b>
5.1.1 STRATEGIES IPSEC .....	75
5.1.2 MISE EN PLACE DE LA STRATEGIE IPSEC .....	75
5.1.3 STRATEGIES IPSEC PREDEFINIES .....	77
5.1.4 ACTIVATION D'UNE STRATEGIE IPSEC .....	81
5.1.5 TEST DE FONCTIONNEMENT .....	81
<b>5.2 DEPLOIEMENT D'IPSEC AVEC ROUTEUR CISCO 2600 .....</b>	<b>82</b>
5.2.1 ETAPES DE CONFIGURATIONS .....	83
5.2.2 DESCRIPTION DES ETAPES DE CONFIGURATIONS .....	84
<b>5.3 DEPLOIEMENT D'IPSEC AVEC LINUX RED HAT .....</b>	<b>86</b>
5.3.1 INSTALLATION ET CONFIGURATION DE STRONGSWAN .....	87
5.3.2 CONFIGURATION .....	88
5.3.3 FICHIER DE CONFIGURATION IPSEC.SECRETS .....	88
5.3.4 FICHIER DE CONFIGURATION IPSEC.CONF .....	89
<b>5.3.5 MODIFICATION DU FICHIER DE CONFIGURATION.....</b>	<b>89</b>
<b>5.3.6 DEMARRAGE DE STRONGSWAN.....</b>	<b>91</b>
<b>5.3.7 COMMANDES UTILES .....</b>	<b>91</b>
<b>5.3.8 FICHIERS DE LOGS.....</b>	<b>92</b>
<b>5.4 CONCLUSION.....</b>	<b>92</b>
<b>CONCLUSION GENERALE .....</b>	<b>93</b>
<b>BIBLIOGRAPHIE.....</b>	<b>95</b>
<b>REQUEST FOR COMMENTS .....</b>	<b>95</b>
<b>WEBLIOGRAPHIE.....</b>	<b>96</b>