

Merike Kaeo



# SÉCURITÉ DES RÉSEAUX

Un guide pratique pour créer  
une infrastructure de réseau sécurisée

CISCO SYSTEMS  
  
CISCO PRESS  
[www.ciscopress.com](http://www.ciscopress.com)

005-235-1

2-005-235-1

# Sécurité des réseaux

Merike Kaeo



CISCO SYSTEMS  
  
CISCO PRESS

  
CAMPUSPRESS  
FRANCE

---

# Table des matières

---

|                                  |          |
|----------------------------------|----------|
| <b>Introduction .....</b>        | <b>1</b> |
| A qui s'adresse ce livre ? ..... | 2        |
| Organisation .....               | 2        |

## Partie I. Notions fondamentales sur la sécurité

|                                                              |           |
|--------------------------------------------------------------|-----------|
| <b>Chapitre 1. Concepts de cryptographie .....</b>           | <b>7</b>  |
| Qu'est-ce que la cryptographie ? .....                       | 8         |
| Cryptage symétrique .....                                    | 9         |
| Cryptage asymétrique .....                                   | 13        |
| Fonctions de hachage .....                                   | 17        |
| Signatures numériques .....                                  | 19        |
| Authentification et autorisation .....                       | 21        |
| Méthodes d'authentification .....                            | 22        |
| Modèles de confiance .....                                   | 22        |
| Espaces de nom .....                                         | 23        |
| Gestion des clés .....                                       | 24        |
| Création et distribution de clés secrètes .....              | 24        |
| Création et distribution de clés publiques .....             | 28        |
| Tiers de confiance .....                                     | 31        |
| Entreprises .....                                            | 32        |
| Aspect politique .....                                       | 32        |
| Facteur humain .....                                         | 32        |
| Résumé .....                                                 | 33        |
| <b>Chapitre 2. Technologies de sécurité .....</b>            | <b>35</b> |
| Technologies d'identification .....                          | 36        |
| Mots de passe sécurisés .....                                | 37        |
| Protocoles d'authentification pour PPP .....                 | 43        |
| Protocoles utilisant des mécanismes d'authentification ..... | 51        |
| FORTEZZA .....                                               | 63        |

|                                                                                |     |
|--------------------------------------------------------------------------------|-----|
| Sécurité dans les couches TCP/IP .....                                         | 65  |
| Protocoles de sécurité de la couche Application .....                          | 65  |
| Protocoles de sécurité de la couche Transport .....                            | 66  |
| Sécurité de la couche Réseau .....                                             | 71  |
| Sécurité dans les couches TCP/IP .....                                         | 78  |
| Technologies d'accès distants sécurisés par réseaux privés virtuels .....      | 79  |
| Protocole L2F .....                                                            | 79  |
| Protocole PPTP .....                                                           | 82  |
| Protocole L2TP .....                                                           | 84  |
| Technologies d'accès distant par réseau virtuel .....                          | 88  |
| Infrastructure de gestion et modèles de distribution de clés publiques .....   | 92  |
| Fonctions d'une infrastructure de gestion de clés publiques .....              | 93  |
| Exemple d'infrastructure de gestion de clés .....                              | 94  |
| Certificats .....                                                              | 95  |
| Standard X.509 .....                                                           | 96  |
| Distribution de certificats .....                                              | 99  |
| Résumé .....                                                                   | 101 |
| <b>Chapitre 3. Contrôle de l'exportation en matière de cryptographie</b> ..... | 103 |
| Aperçu historique de la politique américaine .....                             | 104 |
| Perspectives historiques sur la politique internationale .....                 | 107 |
| Signatures numériques .....                                                    | 118 |
| Preuve juridique d'authenticité .....                                          | 118 |
| Authenticité des signatures écrites .....                                      | 119 |
| Résumé .....                                                                   | 120 |

## Partie II. Stratégies de sécurité d'entreprise

|                                                             |     |
|-------------------------------------------------------------|-----|
| <b>Chapitre 4. Menaces sur un réseau d'entreprise</b> ..... | 123 |
| Types de menaces .....                                      | 124 |
| Accès non autorisé .....                                    | 124 |
| Usurpation d'identité .....                                 | 126 |
| Déni de service .....                                       | 129 |
| Motivation des attaquants .....                             | 130 |
| Vulnérabilités courantes .....                              | 131 |
| Suite TCP/IP .....                                          | 131 |
| Protocole UDP .....                                         | 137 |
| Protocole ICMP .....                                        | 138 |
| Protocole NNTP .....                                        | 140 |

|                                                                                                |            |
|------------------------------------------------------------------------------------------------|------------|
| Protocole SMTP .....                                                                           | 140        |
| Protocole FTP .....                                                                            | 141        |
| Services NFS/NIS .....                                                                         | 142        |
| Système X Window .....                                                                         | 142        |
| Ingénierie sociale .....                                                                       | 143        |
| Résumé .....                                                                                   | 143        |
| <b>Chapitre 5. Politique de sécurité d'entreprise .....</b>                                    | <b>145</b> |
| Commencement .....                                                                             | 146        |
| Gestion des risques .....                                                                      | 148        |
| Evaluation des risques .....                                                                   | 149        |
| Réduction des risques et du coût de la sécurité .....                                          | 156        |
| Cadre fonctionnel d'une politique de sécurité .....                                            | 157        |
| Composants d'un réseau entreprise .....                                                        | 158        |
| Éléments d'une architecture de sécurité .....                                                  | 159        |
| Autres considérations de sécurité .....                                                        | 162        |
| Résumé .....                                                                                   | 163        |
| <b>Chapitre 6. Conception et implémentation d'une stratégie de sécurité d'entreprise .....</b> | <b>165</b> |
| Contrôles de sécurité physique .....                                                           | 166        |
| Infrastructure physique du réseau .....                                                        | 166        |
| Sécurité physique des équipements .....                                                        | 171        |
| Contrôles de sécurité logique .....                                                            | 174        |
| Frontières de sous-réseaux .....                                                               | 175        |
| Contrôle d'accès logique .....                                                                 | 181        |
| Intégrité de l'infrastructure et des données .....                                             | 184        |
| Pare-feu .....                                                                                 | 185        |
| Services de réseau .....                                                                       | 187        |
| Données authentifiées .....                                                                    | 189        |
| Résistance aux attaques courantes .....                                                        | 190        |
| Confidentialité des données .....                                                              | 192        |
| Stratégies et procédures pour le personnel .....                                               | 193        |
| Protection des sauvegardes .....                                                               | 193        |
| Certification de l'équipement .....                                                            | 193        |
| Emploi d'outils portables .....                                                                | 194        |
| Résultats d'audit .....                                                                        | 194        |
| Sensibilisation du personnel à la sécurité .....                                               | 196        |
| Ingénierie sociale .....                                                                       | 197        |
| Résumé .....                                                                                   | 198        |

|                                                      |     |
|------------------------------------------------------|-----|
| <b>Chapitre 7. Gestion d'incidents</b> .....         | 199 |
| Création d'une équipe de réponse aux incidents ..... | 200 |
| Compétences requises .....                           | 201 |
| Détection d'incidents .....                          | 201 |
| Gestion d'incidents .....                            | 203 |
| Définition de la priorité des actions .....          | 203 |
| Evaluation des dommages .....                        | 204 |
| Reporting et procédures d'alerte .....               | 204 |
| Réponse aux incidents .....                          | 206 |
| Documentation des incidents .....                    | 206 |
| Scénarios d'incidents .....                          | 207 |
| Récupération après incident .....                    | 208 |
| Résumé .....                                         | 208 |

### Partie III. Implémentation pratique

|                                                                              |     |
|------------------------------------------------------------------------------|-----|
| <b>Chapitre 8. Sécurité de l'infrastructure de réseau d'entreprise</b> ..... | 213 |
| Identité .....                                                               | 214 |
| Contrôle de l'accès aux équipements de réseau .....                          | 214 |
| Intégrité .....                                                              | 233 |
| Authentification d'image .....                                               | 234 |
| Protection des groupes de travail .....                                      | 234 |
| Authentification de routeurs .....                                           | 235 |
| Filtres de routes et fiabilité du routage .....                              | 237 |
| Confidentialité des données .....                                            | 239 |
| Disponibilité du réseau .....                                                | 240 |
| Fonctions de redondance .....                                                | 241 |
| Protection contre les attaques courantes .....                               | 247 |
| Audit .....                                                                  | 250 |
| Vérification des configurations .....                                        | 250 |
| Surveillance et journalisation de l'activité de réseau .....                 | 250 |
| Détection d'intrusion .....                                                  | 252 |
| Produits d'audit Cisco .....                                                 | 253 |
| Exemple d'implémentation .....                                               | 253 |
| Résumé .....                                                                 | 255 |
| <b>Chapitre 9. Sécurisation de l'accès Internet</b> .....                    | 257 |
| Architecture de l'accès Internet .....                                       | 257 |
| Architecture de routeur filtrant externe .....                               | 259 |
| Filtres Cisco IOS .....                                                      | 260 |

|                                                                     |            |
|---------------------------------------------------------------------|------------|
| Architecture pare-feu .....                                         | 269        |
| Filtrage avancé de sessions .....                                   | 270        |
| Filtrage de contenu d'applications .....                            | 271        |
| Authentification/autorisation d'applications .....                  | 276        |
| Cryptage .....                                                      | 277        |
| Traduction NAT .....                                                | 279        |
| Exemples d'implémentation .....                                     | 283        |
| Pare-feu Cisco IOS .....                                            | 283        |
| Pare-feu PIX avec routeur filtrant Cisco IOS .....                  | 290        |
| Résumé .....                                                        | 301        |
| <b>Chapitre 10. Sécurisation de l'accès distant .....</b>           | <b>303</b> |
| Protection de l'accès distant .....                                 | 304        |
| Authentification des utilisateurs et des équipements distants ..... | 305        |
| Environnements simples d'accès distant .....                        | 306        |
| Environnements complexes d'accès distant .....                      | 310        |
| Autorisation .....                                                  | 315        |
| Autorisation TACACS+ et RADIUS .....                                | 316        |
| Fonctionnalité lock-and-key .....                                   | 321        |
| Authentification/autorisation double .....                          | 327        |
| Comptabilité et facturation .....                                   | 333        |
| Comptabilité TACACS+ et RADIUS .....                                | 333        |
| Facturation centralisée .....                                       | 335        |
| Autres aspects de l'accès distant par réseau virtuel .....          | 336        |
| Tunnel GRE .....                                                    | 337        |
| Technologie de chiffrement Cisco CET .....                          | 338        |
| IPsec .....                                                         | 339        |
| Exemples d'implémentation .....                                     | 341        |
| GRE avec CET .....                                                  | 341        |
| L2TP avec IPsec .....                                               | 346        |
| Résumé .....                                                        | 362        |

## Partie IV. Annexes

|                                                                |            |
|----------------------------------------------------------------|------------|
| <b>Annexe A. Sources d'informations techniques .....</b>       | <b>367</b> |
| Ouvrages sur la cryptographie et la sécurité des réseaux ..... | 367        |
| Ouvrages sur les pare-feu .....                                | 367        |
| IETF (Internet Engineering Task Force) .....                   | 367        |
| Documents sur les stratégies de sécurité de réseau .....       | 368        |

---

|                                                             |            |
|-------------------------------------------------------------|------------|
| Equipes de réponse aux incidents .....                      | 369        |
| Autres sites utiles sur la sécurité .....                   | 369        |
| Informations sur les produits de sécurité Cisco .....       | 369        |
| <b>Annexe B. Directives d'alerte et de prévention .....</b> | <b>371</b> |
| Découverte du problème .....                                | 371        |
| Réactions .....                                             | 371        |
| Investigation .....                                         | 372        |
| Philosophie sur le lieu de travail .....                    | 372        |
| Rédaction d'un plan de sécurité .....                       | 373        |
| Lois et procédures .....                                    | 373        |
| Systèmes informatiques et réseaux .....                     | 374        |
| Employés .....                                              | 374        |
| Méthodes de protection des informations propriétaires ..... | 375        |
| Contrôle des documents .....                                | 376        |
| Contacts par la concurrence .....                           | 377        |
| Personnes responsables .....                                | 377        |
| Procédures de compte-rendu et récompenses .....             | 377        |
| Méthodes de collecte d'informations .....                   | 378        |
| Recherche des points faibles .....                          | 378        |
| Législation relative à la fraude informatique .....         | 379        |
| <b>Annexe C. Numéros de ports .....</b>                     | <b>381</b> |
| <b>Glossaire .....</b>                                      | <b>385</b> |
| <b>Index .....</b>                                          | <b>391</b> |