

Table des matières

Avant-propos	1
Introduction	3
Chapitre 1. Les concepts de base de la sécurité des réseaux.	5
1.1. Introduction.	5
1.1.1. Les objectifs principaux de la sécurité d'un réseau	6
1.1.2. Terminologie de la sécurité informatique	6
1.1.2.1. Terminologie générale.	6
1.1.2.2. Types de pirates	7
1.1.2.3. Codes malveillants	7
1.2. Les types de sécurité réseau	8
1.2.1. La sécurité physique	8
1.2.2. La sécurité logique	9
1.2.3. La sécurité administrative	9
1.3. Les principaux risques liés à la sécurité logique du réseau	10
1.3.1. Les différents types d'attaque réseau	10
1.3.1.1. Les attaques de reconnaissance	10
1.3.1.2. Les attaques du mot de passe	10
1.3.1.3. Les attaques d'accès	10
1.3.1.4. Les attaques du réseau contre la disponibilité	11
1.3.1.5. Les attaques rapprochées	12
1.3.1.6. Les attaques de la relation d'approbation.	12
1.3.2. Les mesures de la sécurité réseau.	12
1.3.3. Les mesures d'audit des vulnérabilités	12
1.4. Travaux dirigés.	13

Chapitre 2. La sécurisation des périphériques réseau	21
2.1. Les types de trafic réseau	21
2.2. La sécurisation du plan de gestion	22
2.3. La sécurisation des mots de passe	22
2.4. L'implémentation des restrictions de connexion	23
2.4.1. La configuration d'une bannière de connexion	23
2.4.2. La configuration des paramètres de connexion	23
2.5. La sécurisation de l'accès par les lignes console, vty et auxiliaire	24
2.5.1. La sécurisation de l'accès par la ligne console et la désactivation de la ligne auxiliaire	24
2.5.2. La sécurisation de l'accès vty avec ssh	24
2.6. L'attribution des rôles administratifs	25
2.6.1. Les niveaux de privilège du système IOS	25
2.6.2. Configurer un niveau de privilège	25
2.6.3. Définir un niveau de privilège par utilisateur	26
2.6.4. Définir un niveau de privilège pour l'accès des lignes console, vty et auxiliaire	27
2.6.5. Sécuriser l'accès à l'aide de la gestion de « vues » et de « super-vues »	27
2.6.5.1. Présentation des vues	27
2.6.5.2. Présentation des super-vues	28
2.6.6. La sécurisation des fichiers de configuration et du système IOS	29
2.6.7. L'utilisation des fonctionnalités de sécurité automatisées	30
2.6.7.1. Présentation	30
2.6.7.2. Configuration	30
2.7. La sécurisation du plan de contrôle	30
2.7.1. Présentation	30
2.7.2. L'authentification MD5	31
2.7.3. Configuration de l'authentification de protocole OSPF	31
2.7.4. Configuration de l'authentification du protocole EIGRP	32
2.7.5. Configuration de l'authentification du protocole RIP	32
2.8. Travaux pratiques	33
Chapitre 3. La supervision d'un réseau informatique	49
3.1. Présentation	49
3.2. Implémenter un serveur NTP	50
3.2.1. Présentation du NTP	50
3.2.2. Fonctionnement du NTP	50
3.2.2.1. Les différents niveaux du NTP	50
3.2.2.2. Les modes de communication du NTP	51
3.2.3. Configuration du protocole NTP	51

3.2.3.1. Configurer un routeur maitre NTP	51
3.2.3.2. Configurer un client NTP	51
3.3. Implémenter un serveur Syslog	52
3.3.1. Présentation du Syslog	52
3.3.2. Fonctionnement du Syslog	53
3.3.2.1. Les niveaux de gravité Syslog	53
3.3.2.2. Le format d'un message Syslog	53
3.3.3. Configurer un client Syslog	54
3.4. Implémenter le protocole SNMP	54
3.4.1. Présentation du SNMP	54
3.4.2. Fonctionnement du SNMP	55
3.4.2.1. Les composants d'un système SNMP	55
3.4.2.2. La structure de la base d'informations de management	56
3.4.2.3. Les différentes versions du SNMP	56
3.4.2.4. Les messages SNMP	57
3.4.3. Configuration du SNMP	58
3.5. Travaux pratiques	58
Chapitre 4. La sécurisation de l'accès de gestion avec AAA	77
4.1. Présentation	77
4.2. L'authentification AAA	78
4.2.1. L'authentification AAA locale	78
4.2.2. L'authentification AAA basée sur un serveur	79
4.3. Les autorisations AAA	81
4.4. La traçabilité AAA	81
4.5. Travaux pratiques	82
Chapitre 5. Utiliser les pare-feu	89
5.1. Présentation d'un pare-feu	90
5.2. Les types de pare-feu	90
5.3. L'implémentation d'un pare-feu	90
5.4. Les différentes stratégies d'un pare-feu	91
5.5. Les pare-feu à base d'ACL	91
5.5.1. Présentation	91
5.5.2. L'emplacement des ACL	91
5.5.3. Les ACL IPv4	92
5.5.4. Les ACL IPv6	93
5.5.5. Recommandation sur les ACL	93
5.6. Les pare-feu à base de zones	94
5.6.1. Présentation	94

5.6.2. Les types de zones de sécurité dans un réseau	94
5.6.3. Les règles appliquées au trafic interzone	95
5.6.4. Terminologie.	96
5.6.5. Configuration d'un ZFW	96
5.7. Créer les zones	96
5.8. Créer les Class-Map.	97
5.9. Créer les Policy-Map pour appliquer les Class-Map.	97
5.10. Définir les paires de zones	97
5.11. Appliquer les mappages de stratégie aux paires de zones	97
5.12. Affecter des interfaces aux zones	98
5.13. Travaux pratiques	98
Chapitre 6. Mettre en œuvre la prévention des intrusions IPS	113
6.1. Présentation d'un capteur.	114
6.2. Les différences entre un IDS et un IPS.	114
6.3. Les types d'IPS	115
6.4. Les solutions IPS de Cisco	115
6.5. Les modes de déploiement de l'IPS	115
6.6. Les types d'alarmes	116
6.7. La détection du trafic malveillant	116
6.7.1. Les modes de détection	116
6.7.2. La détection à base de signatures.	116
6.7.2.1. Définition d'une signature	116
6.7.2.2. Les types de signatures	117
6.7.2.3. Les caractéristiques de ce mode de détection	117
6.7.3. Les autres modes de détection du trafic malveillant.	117
6.7.3.1. La détection à base de stratégies	117
6.7.3.2. La détection à base d'anomalies	118
6.7.3.3. La détection à base de réputation	118
6.8. Les micromoteurs de signatures.	119
6.9. Les niveaux de gravité des signatures	119
6.10. Surveillance et gestion des alarmes et des alertes.	120
6.11. La liste des actions à prendre lors d'une attaque	120
6.12. Configuration de l'IPS IOS.	121
6.13. Les pratiques recommandées.	123
6.14. Travaux pratiques	124
Chapitre 7. Sécuriser un réseau local	137
7.1. Présentation.	137
7.2. Les types d'attaques sur la couche 2	138

7.2.1. Les attaques d'inondation d'adresses MAC	138
7.2.2. L'attaque par usurpation d'adresse MAC	139
7.2.3. L'attaque « DHCP starvation »	139
7.2.4. L'attaque par saut de VLAN	140
7.2.4.1. L'attaque par usurpation de commutation	140
7.2.4.2. L'attaque par double étiquetage	141
7.2.5. Les attaques à base du protocole STP	142
7.3. Les meilleures pratiques de sécurité pour protéger la couche 2	143
7.4. Travaux pratiques	144

Chapitre 8. La cryptographie 157

8.1. Notions de base de la cryptographie	157
8.1.1. Définition	157
8.1.2. Terminologie	158
8.2. Les différentes classifications de la cryptologie	158
8.2.1. La cryptographie classique	159
8.2.1.1. Le chiffrement par substitution	159
8.2.1.2. Le chiffrement par transposition	160
8.2.2. La cryptographie moderne	160
8.2.2.1. Le chiffrement par blocs	160
8.2.2.2. Le chiffrement par flux	161
8.2.3. Chiffrement symétrique et asymétrique	161
8.2.3.1. Chiffrement symétrique	161
8.2.3.2. Chiffrement asymétrique	162
8.3. La gestion des clés	163
8.3.1. Présentation	163
8.3.2. L'échange de clés Diffie-Hellman	163
8.4. Les fonctions de hachage	165
8.5. Les codes HMAC	165
8.6. La cryptographie asymétrique	165
8.6.1. Présentation	165
8.6.2. Fonctionnement	166
8.6.3. Les signatures numériques	167
8.6.3.1. Présentation	167
8.6.3.2. Fonctionnement	167
8.6.4. Les infrastructures à clé publique	169
8.6.4.1. Présentation	169
8.6.4.2. Terminologie	170
8.6.4.3. Les normes PKI	170
8.6.4.4. Les topologies PKI	171
8.7. Travaux pratiques	173

Chapitre 9. Les VPN IPsec	187
9.1. Le protocole IPsec	187
9.1.1. Les objectifs d'IPsec	187
9.1.2. Les protocoles de base d'IPsec	188
9.1.3. Le cadre IPsec	188
9.1.4. L'association de sécurité IPsec	189
9.1.5. Les modes IPsec	189
9.2. Le protocole IKE	190
9.2.1. Présentation	190
9.2.2. Les composants d'IKE	190
9.2.3. Les phases IKE	191
9.2.3.1. La phase 1 de IKE	191
9.2.3.2. La phase 2 de IKE	192
9.2.3.3. Les différences entre les deux versions IKE	192
9.3. La configuration des VPN de site à site	192
9.3.1. Présentation	192
9.3.2. Configuration du VPN IPsec	193
9.4. Travaux pratiques	196
Chapitre 10. Étudier les pare-feux évolués	205
10.1. Les pare-feux Cisco ASA	205
10.1.1. Présentation	205
10.1.2. Les modèles ASA	206
10.1.3. Les modes d'utilisation des équipements ASA	207
10.1.4. Un aperçu sur ASA 5505	207
10.1.5. Les niveaux de sécurité ASA	208
10.1.6. La configuration d'ASA avec CLI	209
10.1.6.1. Les types de licences ASA 5505	209
10.1.6.2. Présentation du CLI sur ASA	209
10.1.6.3. Configuration des interfaces	210
10.1.6.4. Configuration du service DHCP	210
10.1.6.5. Configuration des ACL	211
10.1.6.6. Configuration du service NAT	211
10.1.6.7. Configuration de AAA	213
10.2. Travaux pratiques	214
10.3. La configuration des éléments Cisco avec des outils graphiques	227
10.3.1. Présentation de CCP	227
10.3.2. Présentation de l'ASDM	228
10.3.3. Utilisation de CCP et de l'ASDM	228

10.4. Le pare-feu TMG 2010	228
10.4.1. Présentation.	228
10.4.2. Installation et configuration	228
Bibliographie	261
Index	263