

s o l u t i o n s  
r é s é a u x

F R A N C I S I A  
O L I V I E R M E N A G E R

# Optimiser et sécuriser son trafic IP

Avec la contribution de  
Jean-Marc Barozet,  
Pascal Delprat et  
Olivier Sez nec,  
de Cisco Systems,  
et la collaboration de  
Olivier Salvatori

© Groupe Eyrolles, 2004,

ISBN : 2-212-11274-2

**EYROLLES**



# Table des matières

---

<b>Remerciements</b> .....	VII
<b>Avant-propos</b> .....	IX
<b>Structure de l'ouvrage</b> .....	X
<b>Public visé</b> .....	XII
CHAPITRE 1	
<b>La commutation 4-7</b> .....	1
<b>Définition de la commutation 4-7</b> .....	2
<b>Les services de la commutation 4-7</b> .....	3
La redirection intelligente .....	3
La haute disponibilité .....	8
<b>Concepts et paramètres techniques de la commutation 4-7</b> .....	10
La commutation de niveau 7 .....	11
Les fermes de ressources .....	12
VIP (Virtual IP) .....	12
Persistance des sessions .....	14
Architecture entre parenthèses .....	14
La redondance .....	16
Basculement sans perte de session .....	17

<b>Mise en œuvre de la commutation 4-7</b> .....	17
L'acheminement des paquets .....	18
Transformation des paquets à l'aller .....	19
Transformation des paquets au retour .....	21
<b>Intégration des commutateurs 4-7 dans l'architecture</b> .....	21
Intégration physique du commutateur 4-7 .....	21
Intégration logique IP du commutateur 4-7 .....	23
Redondance de l'infrastructure .....	24
<b>En résumé</b> .....	25

## CHAPITRE 2

<b>Les pare-feu</b> .....	27
<b>Définition d'un pare-feu</b> .....	29
Limites des pare-feu .....	30
Principes d'architecture .....	30
<b>Les mécanismes de filtrage</b> .....	32
Le filtrage statique des paquets .....	32
Le filtrage dynamique, ou stateful .....	34
<b>Typologie des pare-feu</b> .....	35
Les pare-feu proxy .....	35
La technologie Air Gap .....	41
Le bastion .....	45
Les pare-feu hybrides .....	46
Les pare-feu personnels distribués .....	50
<b>La haute disponibilité</b> .....	53
La redondance des pare-feu .....	54
La redondance et l'équilibrage de charge logiciels .....	56
<b>Tester et administrer un pare-feu</b> .....	56
Quand et comment tester ? .....	56
Administrer .....	57
Externalisation des pare-feu ? .....	58
<b>En résumé</b> .....	59

## CHAPITRE 3

<b>Les réseaux privés virtuels (VPN)</b> .....	61
<b>Définition d'un VPN</b> .....	61
<b>Architecture et protocoles</b> .....	66
PPTP (Point-to-Point Tunneling Protocol) .....	66
Cisco L2F (Layer 2 Forwarding) .....	69
L2TP (Layer 2 Tunneling Protocol) .....	69
IPsec .....	71
<b>Les protocoles orientés opérateurs ou très grands comptes</b> .....	78
MPLS (MultiProtocol Label-Switching) .....	79
L2TP v3 .....	85
SSL (Secure Sockets Layer) .....	85
<b>Comparaison des VPN IPsec et de SSL-TLS</b> .....	97
<b>VPN SSL et VPN applicatifs</b> .....	98
Les VPN SSL .....	99
Critères de choix d'un VPN SSL .....	101
<b>En résumé</b> .....	103

## CHAPITRE 4

<b>L'accélération de flux IP</b> .....	105
<b>Les technologies d'accélération IP</b> .....	107
Principes de base de l'accélération IP .....	107
Les techniques génériques d'accélération .....	108
<b>Accélération des flux Web (HTTP et HTTPS)</b> .....	116
Le navigateur Web client .....	117
Les données Web d'entreprise .....	118
L'approche HTTP .....	118
L'approche HTTPS .....	121
L'approche VPN-HTTPS .....	123
<b>Accélération des applications critiques</b> .....	124
<b>En résumé</b> .....	126

## CHAPITRE 5

<b>Détection-prévention d'intrusion et honeypots</b> .....	129
<b>Les différents types d'IDS</b> .....	130
Modes de fonctionnement des IDS .....	132
Où placer l'IDS ? .....	135
Techniques de contournement des IDS par les hackers .....	136
<b>Les IPS, de la détection à la prévention</b> .....	137
<b>Paramétrage et administration des IDS/IPS</b> .....	138
<b>Critères de choix d'un IDS/IPS</b> .....	139
<b>Contrôleurs d'intégrité et honeypots</b> .....	139
Mise en place et configuration d'un honeypot .....	142
Les produits du marché .....	143
<b>En résumé</b> .....	145

## CHAPITRE 6

<b>Les attaques Web, armes absolues des hackers</b> .....	147
<b>Les applications Web</b> .....	148
<b>Fonctionnement d'une attaque Web</b> .....	149
<b>Les attaques sur les langages Web</b> .....	150
Le HTML (HyperText Markup Language) .....	151
Le protocole HTTP (Hypertext Transfer Protocol) .....	152
Les en-têtes HTTP .....	157
HTTPS (HTTP over SSL) .....	160
S-HTTP (Secure-Hypertext Transfer Protocol) .....	163
<b>Les attaques d'URL</b> .....	163
Le codage d'URL .....	166
<b>Les attaques SQL</b> .....	171
Le SQL Injection .....	172
Les attaques SQL indirectes .....	178
<b>Les mesures de prévention</b> .....	181
Les attaques CSS ou XSS .....	184
<b>Les services Web (XML, SOAP, WSDL, UDDI)</b> .....	189
<b>En résumé</b> .....	195

## CHAPITRE 7

<b>Antivirus et lutte contre le Spam</b> .....	197
<b>Typologie des attaques</b> .....	198
Virus, ver et codes malicieux .....	198
Le Spam .....	209
<b>Les outils de défense</b> .....	211
Les antivirus .....	211
Applets Java et contrôles ActiveX signés .....	224
Les outils antispam .....	228
<b>En résumé</b> .....	235

## CHAPITRE 8

<b>Gestion de la performance et administration de la sécurité</b> ....	237
<b>Gestion de la performance</b> .....	237
Missions de la gestion de performance .....	238
Les sources de données .....	240
<b>Administration de la sécurité</b> .....	250
Les outils d'administration SIM .....	250
Fonctionnement d'un SIM .....	251
Améliorations de sécurité de SNMP v3 .....	252
Le protocole syslog d'audit de la sécurité .....	257
<b>En résumé</b> .....	258

## CHAPITRE 9

<b>Gestion de la bande passante</b> .....	259
<b>Méthodologie de gestion de la bande passante</b> .....	260
Analyse des flux de trafic .....	260
Classification des flux .....	260
Politique de gestion des flux .....	264
Supervision et génération de rapports .....	265
<b>Allocation de bande passante et lissage du trafic</b> .....	268
Méthodes de partitionnement .....	269
Description technique des mécanismes de lissage de bande passante .....	270
<b>Mise en œuvre des solutions de gestion de bande passante</b> .....	272
<b>En résumé</b> .....	273

## CHAPITRE 10

<b>Méthodologie de mise en œuvre d'une politique de gestion de trafic IP</b> .....	275
<b>L'infrastructure technique</b> .....	276
Qualification du réseau .....	276
Qualification des applications .....	277
<b>Intégration dans le système d'information</b> .....	279
Capacités architecturales des éléments de GTI .....	279
Étapes d'implémentation .....	281
<b>Métrologie et validation</b> .....	282
Métrologie .....	282
Validation .....	283
<b>Organisation et règles d'exploitation</b> .....	283
<b>En résumé</b> .....	284

## CHAPITRE 11

<b>Étude de cas : sécurisation des accès au système d'information</b> ..	285
<b>Environnement de l'entreprise</b> .....	285
<b>Analyse des besoins</b> .....	286
Authentication, authorization, accounting/audit, administration .....	287
<b>Spécification fonctionnelle</b> .....	291
<b>Architecture technique</b> .....	294
<b>Analyse du trafic</b> .....	297
Administration de la sécurité .....	297
<b>Mise en œuvre</b> .....	298
<b>Validation et recette</b> .....	298
<b>En résumé</b> .....	299

## CHAPITRE 12

<b>Exemple d'architecture Cisco pour l'optimisation des performances et de la sécurité d'un Data Center</b> .....	301
<b>Construction du Data Center</b> .....	302
Position du Data Center dans le réseau d'entreprise .....	303

Architecture du Data Center .....	304
Services du Data Center .....	308
<b>Mise en place de l'infrastructure</b> .....	313
Choix de l'algorithme de Spanning Tree .....	315
Le routage dans un Data Center .....	315
Composants du Data Center .....	318
Le niveau 1 .....	319
Le niveau 2 .....	321
Le niveau 3 .....	324
<b>Mise en place de la sécurité</b> .....	331
MAC Flooding .....	331
ARP Spoofing .....	334
Vulnérabilité des PVLAN .....	337
VLAN Hopping .....	339
Vulnérabilité du Spanning Tree .....	340
Sécurité des Data Center intranet .....	343
<b>Annexes</b> .....	351
<b>Les codes d'erreur de HTTP 1.1 (RFC 2616)</b> .....	351
<b>Questions à se poser lors du choix d'un pare-feu</b> .....	354
<b>Retour sur investissement</b> .....	355
<b>Références</b> .....	356
Chapitre 1 : la commutation 4-7 356	
Chapitre 2 : les pare-feu .....	356
Chapitre 4 : les réseaux privés virtuels (VPN) .....	357
Chapitre 6 : détection-prévention d'intrusion et honeypots .....	358
Chapitre 7 : les attaques Web, armes absolues des hackers .....	358
Chapitre 8 : antivirus, lutte antispam et filtrage de contenu .....	361
<b>Index</b> .....	363