solutions
réseaux

FRANCIS IA
OLIVIER MENAGER

Optimiser et sécuriser son trafic IP

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

ISBN : 2-212-11274-2
EYROLLES

Avant-propos

La crise qui a frappé de plein fouet l'économie mondiale à la fin des années 90 a entraîné dans son sillage l'industrie des réseaux et des télécommunications dans un gouffre dont on ne voit toujours pas l'issue. Avant ce cataclysme économique, ce furent les années de l'exubérance, de l'excès et de la surenchère sous toutes leurs formes.

L'exubérance d'abord, à l'image des jeunes pousses qui naissaient en grand nombre, recevaient des capitaux importants d'investisseurs enivrés par la mode *dot com* et représentaient pour toute l'industrie des réseaux et télécoms les catalyseurs de l'économie mondiale. Le phénomène Internet était à son *summum*. Aujourd'hui, nous savons que le point de non-retour était atteint et que la bulle spéculative à force de gonfler sans précaution finirait par éclater.

À cette belle époque, les investissements en infrastructure technique se faisaient sous le signe de l'excès et de la surenchère. Les réseaux devaient être à très haut débit : les opérateurs investissaient sans compter dans des réseaux flambant neufs employant les technologies dernier cri en optique, et les entreprises revoyaient de fond en comble l'ensemble de leur garde-robe réseau, en basculant tout vers les débits Gigabit. Chacun voulait plus que son voisin et intégrait sans raison justifiée les dernières nouveautés technologiques dans son infrastructure, parfois en complète incohérence avec les besoins de l'entreprise.

C'est dans cet état d'esprit que la qualité de service, ou QoS (Quality of Service), est née et a trouvé rapidement un public fervent. C'était le concept phare de l'époque. Toute entreprise se devait d'avoir son projet de QoS, faute de quoi elle était considérée comme dépassée. On faisait rêver en parlant de multimédia communicant au travers d'infrastructures intelligentes capables d'assurer la convergence voix et données dans un réseau commun et de bout en bout.

Le rêve a fait place à la réalité, et la crise a balayé sur son passage tous les concepts apparus lors de ces glorieuses années. La QoS est partie avec l'eau du bain, faisant place à des notions beaucoup plus terre à terre et raisonnables.

L'heure est à la protection de ses biens informatiques et à la sécurisation accrue de son système d'information. L'important est de préserver ses acquis en attendant la fin de la tempête et le retour des beaux jours. La sécurité informatique est ainsi devenue l'un des rares domaines à croître dans la crise. Les méfaits de cette dernière engendrent chez les entreprises utilisatrices un climat de paranoïa propice à l'investissement en sécurité et haute disponibilité.

Le monde industriel prône la productivité et la rentabilité des entreprises et de leurs employés. Ces derniers doivent générer un retour sur investissement qu'on souhaite toujours plus écourté et important. L'outillage informatique fourni aux employés doit satisfaire cet objectif.

L'application informatique a pour mission d'aider l'employé utilisateur à produire davantage. Afin d'atteindre ce but, des applications sont développées pour correspondre de mieux en mieux au métier de l'entreprise et accroître ses bénéfices. On les nomme « applications critiques métier ».

De plus en plus personnalisée pour s'adapter aux spécificités de fonctionnement de l'entreprise, l'application critique métier n'en est pas moins de plus en plus sophistiquée et parfois plus complexe à maîtriser par les employés. L'enjeu pour l'entreprise est de réussir à convaincre ces derniers d'adopter la nouvelle application. C'est le règne de l'utilisateur. Des critères tels que la convivialité de l'interface graphique, la rapidité et le temps de réponse de l'application ou encore sa robustesse aux pannes sont autant de contraintes qu'il est primordial de considérer pour la réussite de l'insertion de l'application dans le système d'information.

Outre-Atlantique, on commence à parler d'*expérience utilisateur,* c'est-à-dire de qualité d'utilisation de l'application. La QoE (Quality of Experience), ou qualité d'expérience, prend la place de la QoS.

Grande tendance de l'époque actuelle, l'optimisation des applications critiques métier revêt plusieurs facettes technologiques, telles que sécurité, haute disponibilité et performance, qui doivent être affinées selon les objectifs et les contextes d'utilisation. C'est ce qu'on appelle la gestion de trafic IP, et c'est le sujet de cet ouvrage.

Structure de l'ouvrage

Cet ouvrage vise à fournir au lecteur une vision complète du domaine de la gestion de trafic IP. Il traite pour cela aussi bien de l'amélioration des performances que de la sécurité et de la haute disponibilité.

L'ouvrage comporte 12 chapitres et une annexe :

- Les chapitres 1 à 9 décrivent les principales technologies à considérer dans le cadre d'un projet d'optimisation de trafic. Ces chapitres détaillent le vaste panorama des solutions techniques disponibles. Chaque description de solution inclut une analyse des besoins ainsi qu'une mise en évidence des concepts mis en œuvre, des services apportés, des mécanismes intrinsèques et des possibilités d'intégration dans l'architecture réseau.

  Vous verrez qu'il est possible de tenir le pari, réputé antinomique, de donner au système d'information le meilleur niveau de protection et de sécurité possible tout en préservant les performances.

  - Le chapitre 1 présente la commutation 4-7, pilier central autour duquel sont reliés les différents blocs fonctionnels d'optimisation de sécurité de trafic. L'analyse au niveau applicatif effectuée par ce type de commutation permet de rediriger intelligemment les flux vers les éléments d'optimisation adéquats.
  - Le chapitre 2 passe en revue les techniques de filtrage implémentées dans les pare-feu.
  - Le chapitre 3 décrit les solutions de VPN (Virtual Private Network), autant logicielles que matérielles, que ce soit au niveau réseau ou applicatif. Ces solutions permettent de construire de manière sécurisée un maillage de réseau privatif reposant sur Internet.
  - Le chapitre 4 introduit les solutions d'accélération de flux applicatifs qui permettent d'améliorer les temps de réponse de l'utilisateur tout en réduisant la bande passante WAN consommée.
  - Le chapitre 5 couvre les technologies de détection d'intrusion, ou IDS (Intrusion Detection System), qui permettent d'analyser au fil de l'eau les flux applicatifs dans le but de parer à toute tentative d'intrusion.
  - Le chapitre 6 recense les parades aux attaques qui agissent au niveau applicatif.
  - Le chapitre 7 détaille les techniques de lutte contre les attaques applicatives, telles que virus, vers, Spam, etc., ainsi que les attaques par insertion dans le flux applicatif.
  - Le chapitre 8 analyse les aspects techniques de l'administration de la sécurité et de la performance du système d'information.
  - Le chapitre 9 se penche sur la gestion de la bande passante en tant que solution d'amélioration de la performance des applications critiques.

- Le chapitre 10 présente une méthodologie de mise en œuvre d'un projet d'optimisation de trafic IP en s'appuyant sur des exemples de réalisation. Une méthodologie de réalisation est explicitée incluant des recommandations sur la validation et l'organisation à mettre en place pour réussir le projet informatique. L'accent est mis sur la phase d'analyse, à la fois qualitative et quantitative. La qualification de l'environnement existant est une étape primordiale pour le succès de l'intégration de nouveaux éléments d'optimisation de la sécurité et de la performance.
- Les chapitres 11 et 12 donnent deux exemples de mise en œuvre et d'implémentation d'optimisation.
  - Le chapitre 11 traite par l'exemple de l'accès sécurisé au système d'information, une problématique répandue dans les grandes entreprises. Nous montrons au travers du cas de l'entreprise factice Martin SA que la politique de sécurité évolue en fonction des caractéristiques des ressources à mettre à disposition et des utilisateurs qui ont besoin d'y accéder.
  - Le chapitre 12 présente un exemple d'implémentation par le constructeur Cisco de la sécurisation du trafic IP. Il nous a en effet paru instructif de connaître le point de vue d'un constructeur sur la question de l'optimisation de la performance et de la sécurité. Nous avons sollicité pour cela le seul constructeur pouvant prétendre fournir des solutions couvrant le plus grand nombre de thèmes abordés dans cet ouvrage. Jean-Marc BAROZET, Pascal DELPRAT et Olivier SEZNEC, de Cisco Systems France, ont accepté de relever le défi.

- L'annexe regroupe les codes d'erreur HTTP, ainsi que les critères de choix d'un pare-feu, une description de la notion de « Retour sur Investissement », et une liste d'ouvrages et de sites de référence sur les sujets couverts dans le livre.

Public visé

Cet ouvrage s'adresse en premier lieu aux responsables du système d'information de l'entreprise. Les domaines technologiques couverts étant la performance et la sécurité des réseaux, tous les ingénieurs techniques évoluant dans ces secteurs y trouveront également intérêt.

Il servira en outre de référence aux étudiants qui souhaitent enrichir leurs connaissances techniques en matière d'optimisation de la performance et de la sécurité des réseaux.