



ContentKeeper Technologies - Vue d'ensemble du produit *ContentKeeper WebFiltering*

Introduction

ContentKeeper technologies a mis au point un produit qui permet de limiter l'accès à l'Internet de façon facile et dynamique. Il aide les organisations à contrôler l'utilisation de l'Internet par le personnel. Il en remet sa gestion à la direction, permettant ainsi une utilisation de l'Internet plus efficace et rentable.

ContentKeeper a gagné le prix Network/Interop du "meilleur nouveau produit d'entreprise 2002" et a reçu une bonne évaluation dans la fameuse revue américaine "Network Computing".

Le produit est installé un peu partout dans le monde, dans les départements du gouvernement australien, chez certains fournisseurs d'Internet (ISP), dans de larges corporations américaines et européennes aussi bien que dans plusieurs établissements scolaires.

Pourquoi limiter l'accès à l'Internet?

Pour pouvoir faire des économies significatives en réduisant:

- 1) le temps perdu par le personnel à naviguer sur des sites non nécessaires
- 2) les coûts et le trafic d'Internet en limitant l'utilisation à des fins d'affaires seulement
- 3) les probabilités de poursuites judiciaires en lieu de travail ainsi que la publicité défavorable et coûteuse qui s'ensuit.

Gaspillage de temps par le personnel

Beaucoup d'organismes se rendent compte du problème relié à l'utilisation de l'Internet, autre que pour affaires, par le personnel, mais n'ont pas, jusqu'à maintenant, analysé l'issue pour savoir ce que sont réellement les implications.

Des études faites suggèrent que le personnel perde, en moyenne, plus d'une heure à naviguer le jour sur des sites sans relations avec le travail.

Cela signifie par que pour une organisation de 2000 employés payés en moyenne \$60 l'heure, le coût est à peu près \$120.000 jour ($\60×2000) ou \$28,8 millions par année (à 240 jours ouvrables par année). Même pour une plus petite organisation de 50 employés au taux horaire de \$50, le coût serait approximativement \$2.500,00 par jour ($\50×50) ou \$600.000 par année.

ContentKeeper fournit l'outil pour mieux gérer ces coûts. **L'épargne peut-être substantielle.**

Gestion du trafic Internet

La navigation sur Internet utilise des ressources physiques qui sont limitées. Par exemple, la quantité d'information qui peut circuler à tout instant est plafonnée, elle a un débit maximum (en anglais "bandwidth"). L'utilisation de cette ressource est un autre secteur où *ContentKeeper* peut aider à faire des économies.

Le personnel aux emplacements non filtrés peut naviguer n'importe où, télécharger de la musique, écouter la radio en ligne, regarder une émission ou simplement employer les ressources via l'écran de sauvegarde ("screen saver"). Le coût inclut non seulement le prix pour fournir ce service non productif mais aussi le coût de ne pas pouvoir se servir de la bande disponible pour affaires.

ContentKeeper permet de gérer les emplacements et les types d'emplacements consultés tout comme les types de services utilisés par le personnel. En limitant l'écoute d'émissions et le téléchargement de dossiers strictement à des emplacements d'affaires l'épargne peut être considérable. Plusieurs emplacements ont rapporté une épargne de plus de 50% grâce à *ContentKeeper*. Dans la plupart des cas cette épargne a été immédiate dès l'installation.

Poursuites judiciaires

L'Internet contient beaucoup de sites pornographiques. Leur nombre croît à un taux effarant et est aisément mis à la disposition de n'importe quel utilisateur non filtré d'Internet.

Le personnel qui accède à de tels emplacements peut, en disséminant volontairement ou non ce matériel à d'autres membres du personnel, créer des situations délicates qui nécessiteront une perte de temps et/ou d'argent supplémentaire à l'organisation. Les cours juridiques de plusieurs pays considèrent de plus en plus que l'employeur se doit de protéger les employés contre de telles situations.

La pornographie infantile est illégale dans la plupart des juridictions et est généralement considérée fortement blessante. La publicité défavorable produite par un tel incident peut être extrêmement préjudiciable à n'importe quelle réputation produisant des coûts directs et indirects en plus de ceux des procédures légales importantes.

Une vue d'ensemble

ContentKeeper fournit l'outil pour une meilleure gestion des coûts d'accès et d'utilisation de l'Internet.

Il permet au gestionnaire de spécifier le type des sites Internet consultés individuellement et/ou par catégorie.

Il permet de contrôler les types de services Internet utilisés, soit les téléchargements de dossier, les émissions audio et vidéo et autres.

Il permet aux organismes de développer et d'imposer leurs propres politiques d'utilisation de l'Internet.

Les politiques de filtrage peuvent être appliquées à différents utilisateurs, à différents groupes d'utilisateurs, à des réseaux et/ou à différentes adresses ou groupes d'adresses Internet (IP)

Chaque politique définit son propre ensemble d'utilisateurs ainsi que leurs filtres par catégorie et/ou par URL, les rapports produits de même que les types de fichiers téléchargeables.

L'accès à l'Internet peut-être restreint en bloquant directement ou être permis après en avoir averti l'utilisateur (supervision) ou être autorisé après authentification. On peut également agir en fonction de l'heure pour permettre, par exemple, d'avoir libre cours à l'Internet seulement après les heures de travail. On peut aussi définir des règles générales qui puissent être modifiées par des règles particulières.

On peut employer les règles standard de blocage et ses écrans d'avertissement et d'authentification ou créer ses propres écrans qui puissent décrire, par exemple, les politiques d'utilisation de l'Internet de la compagnie.

ContentKeeper fournit même le code HTML qui peut être utilisé à ces fins.

Technique

ContentKeeper utilise à la fois une liste de contrôle contenant des millions d'adresses URL (pages web) classifiées par catégorie et un engin d'analyse et de classification qui permet le blocage instantané de sites inconnus indésirables. Des milliers de nouveaux sites sans intérêt pour les affaires sont créés tous les jours à un taux toujours croissant. Des hyperliens à ces nouveaux emplacements sont souvent envoyés aux employés dans le courriel (spam) de façon continue.

Pour combattre ce fléau, *ContentKeeper* met automatiquement à jour sa liste de contrôle sur une base HORAIRE. Tout système de filtrage qui met à jour de nuit, de façon hebdomadaire ou tous les quinze jours est pratiquement inefficace contre les hyperliens d'URL qui arrivent sans arrêt par courriel.

ContentKeeper analyse les liens au fur et à mesure qu'ils sont découverts. Ainsi, un nouveau site est répertorié et disséminé à tous les clients *ContentKeeper*, souvent dans l'heure qui suit. Ces mises à jour sont fournies grâce à une technologie sécuritaire conçue de façon à minimiser l'impact sur la performance du réseau.

ContentKeeper emploie une technologie de filtrage dite de "collaboration en circuit fermé", en instance de brevet aux USA, qui assure que *ContentKeeper* soit supérieur dans sa capacité à contrôler l'accès dans le monde rapidement changeant de l'Internet. Ce filtrage est conçu pour rassembler, analyser, classer, éditer et distribuer les adresses de sites Web dans le monde entier.

Les unités de *ContentKeeper* sont conçues pour appeler le centre de données de *ContentKeeper* périodiquement pour recevoir les mises à jour de la liste de contrôle d'URLs nouvellement découverts et traités. Pendant ce processus, tous les nouveaux URLs suspects découverts localement sont envoyés au Centre de données pour une soumission anonyme à nos engins d'analyse et de catégorisation. Les sites qui sont dans une des catégories de contrôle sont inclus dans la nouvelle liste de contrôle et envoyés à chaque unité de *ContentKeeper* dans le monde.

Ceci signifie que lorsqu'un utilisateur de New York découvre, par exemple, un nouvel emplacement de pornographie, les utilisateurs de *ContentKeeper* à Sydney, Australie (et ailleurs) bénéficieront de cette découverte, normalement dans l'heure qui suit.

Cette technologie de filtrage est également utilisée pour aider à maintenir et éditer la liste existante de contrôle. Les administrateurs de *ContentKeeper* dans le monde entier ont la capacité de reclassifier n'importe quel site localement. Les sites localement reclassifiés sont envoyés de nouveau au centre de données pour une révision manuelle et correction au besoin. Ce système de filtrage assure que la liste de contrôle de *ContentKeeper* soit de meilleure qualité.

Avec une telle méthode, (analyse en temps réel et liste de contrôle) le système s'ajuste rapidement aux emplacements connus et consultés par le personnel local.

Plus longtemps *ContentKeeper* est utilisé, plus il devient efficace.

ContentKeeper peut manipuler des emplacements de 25 utilisateurs aussi facilement que des centaines de milliers. Le système a été conçu pour supporter un gros trafic, sans erreurs, avec une grande disponibilité. Même ceux à charge balancée.

ContentKeeper a été certifié par l'autorité australienne fédérale ABA à l'usage d'ISPs et d'autres organismes, comme système de filtrage principal pour répondre aux exigences de la radiodiffusion. La liste standard de contrôle de *ContentKeeper* contient la liste officielle de l'ABA.

ContentKeeper a été conçu de façon à réduire au minimum l'administration et l'entretien. Les mises à niveau de liste et de logiciel de contrôle sont manipulées automatiquement.

Le centre de données est une partie essentielle du service de *ContentKeeper*. Il rassemble, compile, analyse, classe et distribue des sites par catégorie sans arrêt.

Les moteurs d'analyse, les araignées et le logiciel qui les conduit sont constamment améliorés pendant que de nouvelles techniques sont développées.

C'est là où tout le traitement principal se produit. Notre but est de produire la meilleure qualité et la liste de contrôle la plus précise possible.

ContentKeeper fonctionne par lui-même. Il se présente au réseau comme un pont transparent Ethernet (aucune adresse IP sur les 2 ports de pont) ce qui enlève toute incompatibilité (avec des serveurs de procuration, des pare-feu (firewalls), des redirigeurs (routers), etc.) et en fait une unité pratiquement à l'épreuve des pirates.

Ceci rend son installation simple et rapide: aucune reconfiguration de réseau, aucune modification de configuration d'ordinateur, aucun logiciel à charger sur un système de production existant, avec tous les problèmes d'incompatibilité et de fiabilité qui peuvent en découler.

Elle enlève également la charge de filtrage aux serveurs, aux pare-feu (firewalls) et de procuration (proxy) leur permettant de se consacrer à leurs vrais travaux de façon plus rapide et efficace. Ceci a comme conséquence habituelle d'avoir un accès plus rapide à l'Internet.

La gestion du système s'effectue entièrement par navigateur. On y configure usagers, adresses, groupes et politiques de filtrage.

Les changements aux politiques et aux arrangements de *ContentKeeper* se produisent instantanément sans rupture de réseau ou de nécessité de remettre en marche des services ou de passer par un long rechargement des données de la liste de contrôle en mémoire.

Installation

Il est facile d'installer *ContentKeeper*. Son enregistrement se fait de façon automatique aussitôt activé. Une fois relié à l'Internet le système s'activera de lui-même. Aucune intervention humaine n'est requise.

Fidélité

ContentKeeper a aussi un module facultatif de haute disponibilité (HAM pour *High Availability Module* en anglais)

Ce module est un commutateur électromécanique (sur une carte standard PCI) qui assure la connectivité du réseau même en cas de défaillance du système, qu'elle soit matérielle, logicielle ou externe (ex: panne de courant)

Le logiciel est également robuste. Un programme incorporé surveille et vérifie le système sans arrêt de façon à corriger des erreurs mineures et rapporter son état au HAM pour assurer que le système soit entièrement opérationnel à tout instant.

Matériel requis

ContentKeeper fonctionne sur un PC dédié de classe Pentium (Intel) de 1.2GHz ou mieux, roulant RedHat Linux (versions 7,1, 7,2, ou 7,3), avec 3 cartes NIC IntelPro100s et 500 Mg de mémoire.

Il se présente au réseau comme un pont transparent Ethernet (aucune adresse IP sur les 2 ports de pont) ce qui enlève toute incompatibilité avec les serveurs de procuration (proxy servers), les pare feu, etc.)

Ceci rend l'installation très simple et rapide (aucune reconfiguration d'adresse IP ou de PC) Toute la gestion des politiques de filtrage se fait par navigateur et que ce soit pour l'utilisateur, par adresse IP ou par groupe.

L'abonnement annuel de *ContentKeeper* inclut un permis de logiciel, les mises à jour de liste de commande, les mises à jour du logiciel et le soutien qui se fait par téléphone, fax et courriel.

Particularités de *ContentKeeper* (août 2002)

- Compatible avec les environnements Microsoft, Novell, Unix et Linux gérés en réseau
- Économies et Avantages importants
- Facile à installer et à gérer
- Combinaison de Liste de contrôle et blocage en temps réel
- Reportage immédiat et historique
- Liste de contrôle contenant des millions d'URLs
- Conçu pour une disponibilité constante et débit élevé
- Gestions de politique de filtrage par utilisateur, groupe et adresse IP définies individuellement et/ou par défaut
- Traitement, analyse, catégorisation et reclassification des URLs au centre de données de ContentKeeper
- Conception Basée sur un pont transparent Ethernet à l'épreuve des pirates
- Installation facile sans reconfiguration de PC ni changement d'adresse IP
- Compatible avec n'importe lequel serveur, pare-feu, serveur de procuracy, dispositifs de cache, les routeurs, etc.
- Filtrage collaboratif pour la collection, l'analyse, la catégorisation et l'édition des URLs
- Capacité à surveiller et contrôler l'accès à l'Internet
- Blocage et déblocage instantané d'URLs avec caractères masqués (pattern)
- Bloque les URL qu'ils soient représentés par domaine, URL ou adresse IP
- Contrôle la vidéo et l'audio en ligne, le téléchargement de musique et celui de gros dossiers
- Gestion du téléchargement de dossiers par type de dossier
- Filtrage par usager, groupe, adresse de réseau et masques
- Blocage automatique de nouveaux sites indésirables
- Mises à jour horaires de liste de contrôle
- Mises à jour automatiques du logiciel
- Indépendant du système d'exploitation utilisé.
- Compatible avec les pare-feu, les serveurs de procuracy et tout autre dispositif basé sur des adresses IP
- Totalement indépendant
- Réduit la charge des pare-feu et des serveurs de procuracy
- Entièrement configurable par l'utilisateur localement ou à distance
- Plusieurs modes de blocage
- System d'enregistrement entièrement automatisé (sans besoin d'intervention humaine)
- Suivi des mises à jour de la base de données, de la connectivité de réseau et du statut de système à l'écran
- Suivi de l'activité Internet par site et de l'utilisation du réseau à l'écran
- Suivi du blocage de sites et de fichiers à l'écran
- Surveillance et rapports d'activité
- Rapports d'activité de téléchargement et de prises de copies de secours (backup) disponibles
- Rapports des politiques de filtrage disponible
- Tous les rapports sont disponibles à l'écran
- Possibilité de surnommer les catégories
- Politiques par default
- Politiques globales pour faire des changements instantanés
- Clonage de politique possible
- Filtrage spécifique sur un ou plusieurs ports
- Possibilité de mettre le filtrage en fonction sur une base individuelle

- Exemples de pages HTML pour pouvoir faire ses propres écrans
- Reclassification locale de nouveaux URLs instantanée
- Soumission automatique des URLs localement reclassifiés au Centre de données pour vérification manuelle et reclassification
- Possibilité de backup/restore partiel ou total
- Module optionnel de haute disponibilité, entièrement configurable par fureteur
- Ponts configurables à l'écran
- L'abonnement annuel inclut le permis de logiciel et ses mises à jour, les mises à jour de la liste de contrôle, ainsi que le support technique.

NOTA: Les marques de fabrique et les marques déposées Microsoft, Novell etc. sont la propriété de ces organismes respectifs.

Glossaire

- **Bandwidth** **bande passante, débit**
désigne le débit d'une ligne de communication.
- **Bridge** **pont**
Equipement effectuant une conversion de protocoles, par exemple pour raccorder des réseaux Ethernet et Token Ring
- **Browser** **fureteur / navigateur**
Logiciel client permettant de se déplacer parmi les différents sites du Web, d'afficher des images, d'extraire et d'imprimer des fichiers, et parfois d'entendre des documents sonores (suivant le logiciel et sa version)
- **Firewall** **pare-feu**
Machine ou programme placé entre l'Internet et un réseau IP privé afin de renforcer la sécurité de ce dernier
- **Gateway** **passerelle**
Equipement capable d'effectuer une conversion de certains protocoles de communication
- **Hacker** **pirate**
Terme désignant une personne qui s'introduit illégalement dans un système informatique, souvent dans un but malveillant
- **Router** **routeur**
Equipement destiné à acheminer des paquets de données dans un réseau
- **Uniform Resource Locator (URL)** **(adresse) URL**
Syntaxe employée sur le WWW pour spécifier la localisation physique d'un fichier ou d'une ressource se trouvant sur l'Internet