terbeke
Fresh Food Group

Présentation
Pays ou région : Belgique
Secteur d'activité : Aliments frais

Profil de l'entreprise
Ter Beke, basé à Waarschoot, en Belgique, est l'un des principaux fournisseurs de viandes tranchées et de repas préparés réfrigérés de l'UE. Le groupe compte neuf sites industriels en Belgique, aux Pays-Bas et en France, et emploie environ 1 850 personnes. En 2011, Ter Beke a réalisé un chiffre d'affaires de 403,7 millions d'euros. Ter Beke est coté à Euronext Bruxelles.

Contexte
Depuis longtemps, Ter Beke s'appuie sur un environnement de serveurs terminaux Microsoft Terminal Services, comptabilisant au total huit serveurs centralisés.
Quatre serveurs Citrix XenApp 6.5 sont centralisés à Waarschoot, et plusieurs serveurs terminaux natifs sont disséminés dans les différentes usines du groupe en Europe. En 2011, l'entreprise a commencé à envisager une mise à jour de son système afin de générer des économies, de simplifier la gestion et d'améliorer la convivialité de son environnement.

Solution
Les appliances WatchGuard associées à des services de sécurité UTM (Unified Threat Management)

Avantages
- Disponibilité ininterrompue des applications d'entreprise
- Simplicité d'application des stratégies de sécurité aux individus et aux groupes
- Outils de reporting montrant clairement et en permanence ce qui se passe sur le réseau
- Economies significatives

Ter Beke consolide la sécurité de son réseau Terminal Server/Citrix grâce à WatchGuard

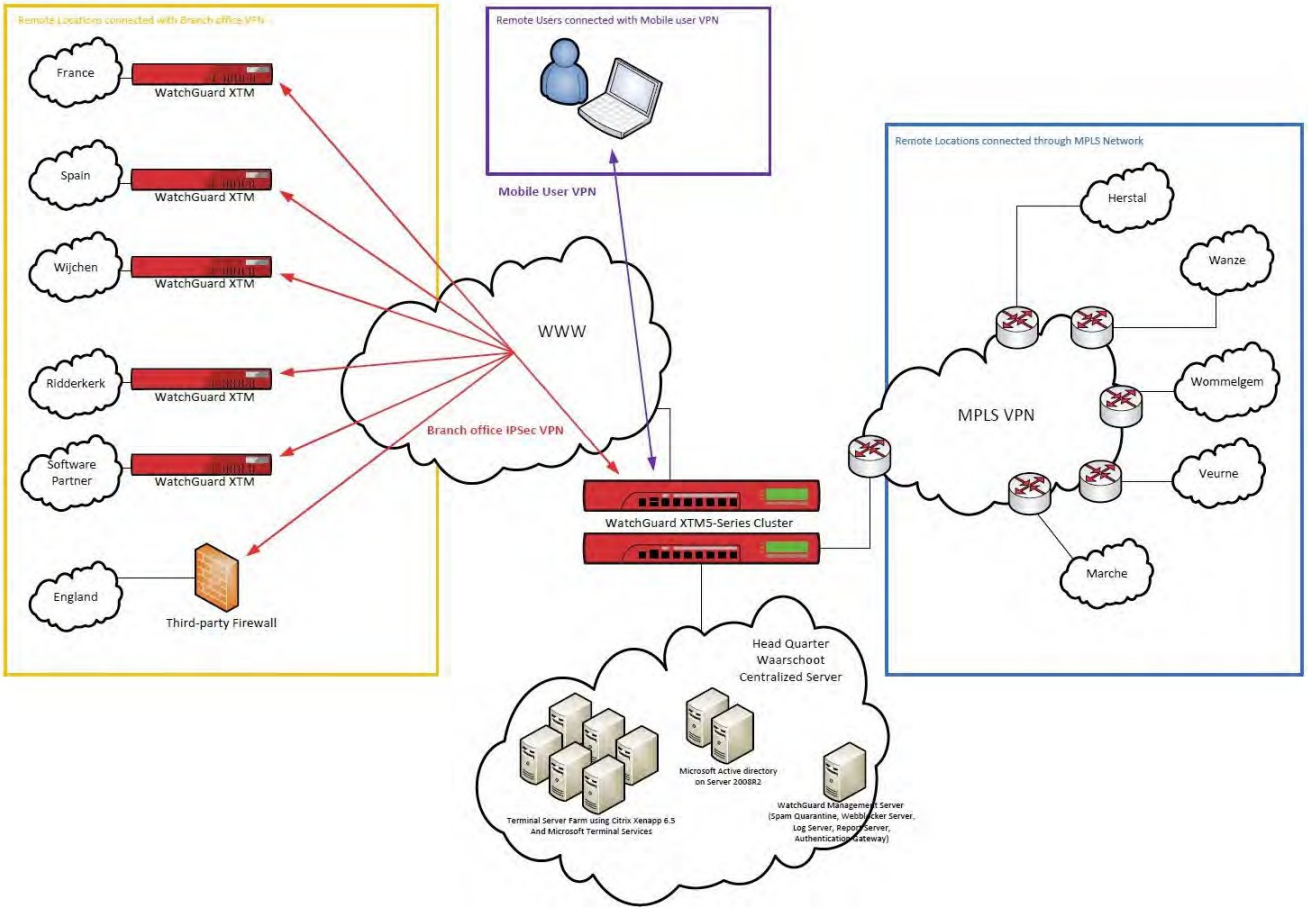
« Nous avons réalisé des économies considérables grâce à la consolidation, notamment sur l'antispam et le filtrage d'URL : pour 500 utilisateurs concurrents cela représente près de 10 000 euros par an »

– Marc Decroos, Directeur informatique et réseau

Le contexte
Ter Beke est un groupe belge innovant spécialisé dans les aliments frais qui commercialise sa ligne de produits dans 10 pays européens.
Le groupe emploie environ 1 850 personnes et se positionne essentiellement sur deux segments : les viandes froides en tranches et les repas préparés réfrigérés. Le réseau interne associe Citrix et des serveurs terminaux. En d'autres termes, des clients légers. Cependant, Ter Beke se trouvait dans l'obligation de mettre en œuvre des stratégies de sécurité pour l'ensemble des employés, sur chaque poste de travail. Les appliances pare-feu WatchGuard ont fourni la solution.

Le défi
L'informatique de l'ensemble du groupe Ter Beke est centralisée à Waarschoot, où est également hébergée la majorité des applications. L'association d'un nuage MPLS privé et de plusieurs VPN sur Internet permet d'assurer les connexions entre les sièges et les sites distants. Ter Beke s'appuie depuis environ 10 ans sur des pare-feu WatchGuard pour la protection de son trafic Internet (deux appliances WatchGuard XTM Série 5 clustérisées à Waarschoot et des appliances XTM Série 2 dans pratiquement tous les sites).

WatchGuard



Terminal Server et Citrix

Ter Beke s'appuie depuis longtemps sur un environnement de serveurs terminaux Microsoft Terminal Services, comptabilisant au total 8 serveurs centralisés. Quatre serveurs Citrix XenApp 6.5 sont centralisés à Waarschoot, et plusieurs serveurs terminaux natifs sont disséminés dans les différentes usines du groupe en Europe. En 2011, l'entreprise a commencé à envisager une mise à jour de son système afin de générer des économies, de simplifier la gestion et d'améliorer la convivialité de son environnement.

Marc Decroos est Responsable des systèmes et des réseaux de Ter Beke depuis 15 ans. Il explique : « La multiplicité des applications et des serveurs terminaux employés sur les différents sites nous a poussé à rechercher une solution plus conviviale. Après tout, ce n'est pas à l'utilisateur de déterminer à quel serveur il doit se connecter pour accomplir certaines tâches bien précises. Nous avons opté pour Citrix, afin que l'utilisateur puisse travailler avec toutes ses applications via de simples icônes, quel que soit l'endroit où l'application s'exécute et où l'utilisateur se trouve. » Le déploiement de la solution Citrix est déjà bien avancé et l'objectif à terme consiste à en équiper tous les postes de travail, y compris ceux employés dans les différentes usines de production.

Jorgen De Wael, Ingénieur système chez Ter Beke, précise : « Nous avons commencé par une simple opération de centralisation. Tous les serveurs terminaux et de données des différents sites ont été transférés à Waarschoot. Puis, tous les serveurs terminaux ont été convertis en environnement Citrix s'exécutant sur Windows 2008/R2. » Un programme complet de nettoyage a alors été mis en place, et toutes les solutions ponctuelles (antivirus, filtrage Web, antispam) ont été regroupées au sein d'une seule solution WatchGuard UTM centralisée. « Nous avons ainsi pu économiser l'abonnement antispam payé à notre fournisseur WAN et supprimer la licence dédiée à notre coûteuse solution dédiée de filtrage d'URL. Nous avons également économisé de l'argent sur les serveurs associés, qui étaient de fait devenus superflus. Tout est désormais regroupé au sein de la plate-forme WatchGuard », précise Marc Decroos.

Les défis

L'introduction de Citrix a généré un certain nombre de problèmatiques. Marc Decroos et Jorgen De Wael souhaitaient éliminer le serveur de filtrage d'URL afin de bénéficier d'une surveillance bien plus efficace au sein du domaine du pare-feu. Jorgen De Wael expliquait : « Notre solution de filtrage d'URL était un proxy Web, ce qui signifiait en clair que tout le trafic Web transitait par un serveur ISA. Ce qui posait problème parce que certaines applications établissaient leurs propres connexions avec l'extérieur, et nous devions donc appliquer des règles spécifiques. Avec l'ancienne association du filtrage d'URL et du serveur ISA, nous avions en outre besoin de deux composants pour une seule et même fonctionnalité. Ce qui n'était pas très efficace. Nous souhaitions dans l'idéal que ce filtrage s'effectue sur la plate-forme WatchGuard, en périphérie du réseau. Mais avec des solutions de type WatchGuard, cette approche faisait apparaître une complication supplémentaire liée aux serveurs terminaux : dans l'ancien environnement de pare-feu, nous n'étions pas capables de voir quel utilisateur visitait quels sites Web, donc nous n'étions également pas capables d'appliquer des règles spécifiques. »

Il s'agissait là d'un problème que Jorgen De Wael n'avait pas avec le serveur ISA. « Ici, à Waarschoot, nous comptons environ 40 utilisateurs par serveur terminal. Pour introduire des stratégies de sécurité distinctes par employé ou par groupe partageant la même adresse IP dans un environnement Terminal Server, nous devions être capables de les analyser au sein du pare-feu. Si le trafic transite via un proxy Web, alors le premier utilisateur arrivant sur le serveur terminal détermine le groupe auquel appartiennent tous les autres utilisateurs de ce serveur, parce que le pare-feu les considère tous comme un même utilisateur. Cette situation n'était pas tenable » poursuit Jorgen De Wael.

Outre le fait qu'il fallait deux composants pour une seule fonctionnalité et que le proxy de l'ancienne solution de filtrage d'URL générait des latences, il y avait un autre problème majeur : le proxy Web était incapable d'interagir avec certaines applications. « Parfois, un certain filtre devenait soudain actif, et à la place d'un utilisateur autorisé bien précis, une session anonyme apparaissait. De fait, nous devions régulièrement appliquer au pare-feu des exceptions IP afin que les utilisateurs soient de nouveau capables de bénéficier d'un accès extérieur complet, sans être identifiés. Ce n'était pas une démarche sécurisée et cela prenait énormément de temps. »

WatchGuard et Citrix : le couple parfait

La collaboration prévue entre l'environnement Citrix et Terminal Server de Ter Beke et WatchGuard a tout d'abord connu des débuts difficiles.
« La première implémentation de Terminal Services sur l'ancienne version n'a franchement pas été un succès. L'UTM fonctionnait correctement, mais pas le single sign-on (SSO), » précise Marc Decroos.

Alors que la licence de filtrage d'URL de Ter Beke avait presque expiré, aucune nouvelle version avec single sign-on pour Terminal Services n'avait été lancée à l'époque. Il existait, d'après Jorgen De Wael, une version de prévisualisation qui était testée de façon étendue en collaboration avec WatchGuard Benelux.

« En mars 2012, sur les conseils de WatchGuard Benelux, nous avons décidé de la commander quoi qu'il en soit, car la licence de notre solution de filtrage d'URL expirait en mai et nous ne voulions pas continuer à fonctionner encore une année avec une solution ponctuelle. WatchGuard nous a alors promis que nous aurions une solution totalement mature et fonctionnelle à cette date. Et WatchGuard a tenu parole. »

Un agent WatchGuard par serveur Citrix ou terminal contrôle désormais chaque utilisateur associé à une session et assure l'identification personnelle de chaque utilisateur pour le compte du pare-feu, ce qui rend possible l'application de règles de sécurité spécifiques à la périphérie du réseau.

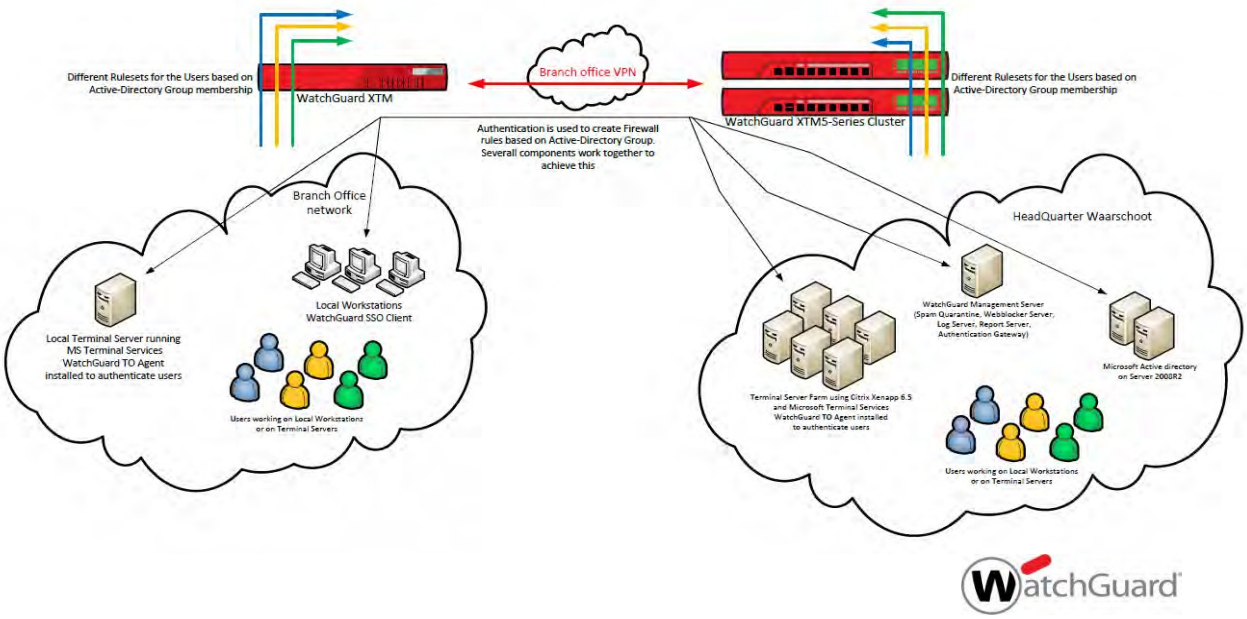
« Pour les processus ERP, certains employés doivent lancer une session avec nous à Waarschoot, mais ils doivent également utiliser Outlook et Office, et certains utilisent également des applications spécifiques liées à la production en usine. Comme Ter Beke peut également utiliser son propre agent par serveur et par région, un modèle distribué s'est mis en place. Ter Beke a en fait besoin d'un environnement Active Directory centralisé qui englobe tous les utilisateurs en Europe. Waarschoot dispose également d'une unique passerelle XTM centralisée redondante avec laquelle tous les agents Terminal Server communiquent, » précise Jorgen De Wael.

Des stratégies individuelles

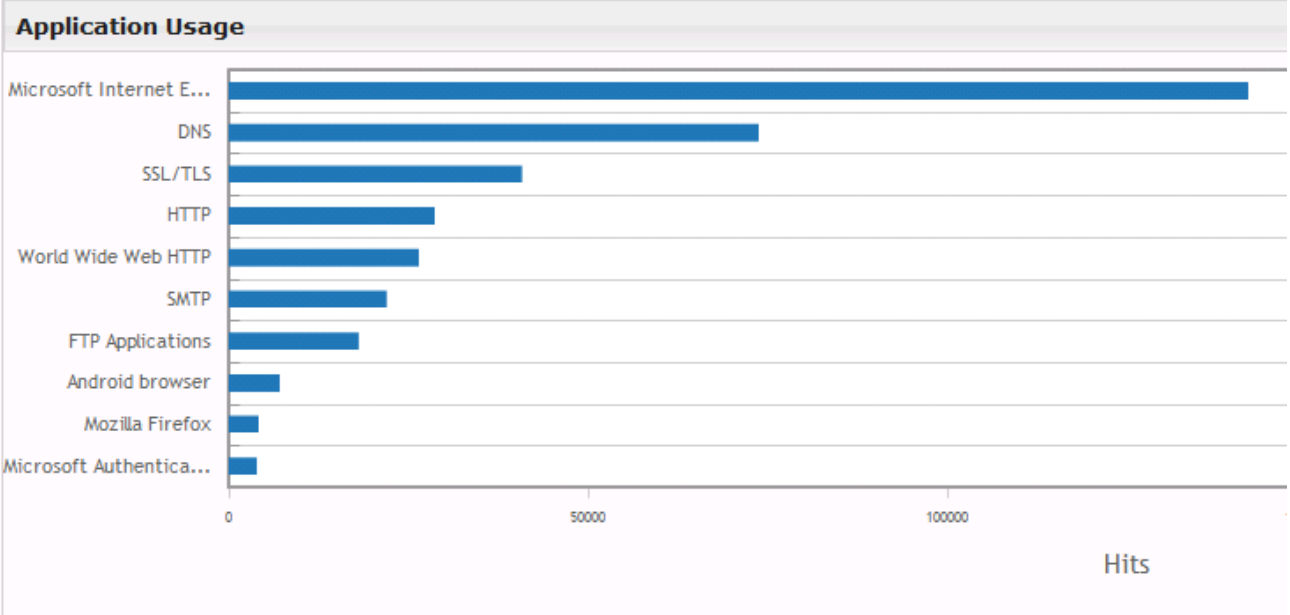
Sur les 1 850 employés que compte Ter Beke, environ 400 utilisent au quotidien des postes de travail ou des ordinateurs portables.
Terminal Server est utilisé sur plusieurs sites de l'entreprise. Par exemple, par les employés qui utilisent des scanners manuels et les conducteurs de chariots élévateurs dans les usines de production et les entrepôts. Ils ne disposent cependant pas de connexion Internet.

Marc Decroos et Jorgen De Wael peuvent décider pour chaque poste de travail ce que l'utilisateur peut et ne peut pas faire sur Internet. Il leur suffit pour cela de créer des règles spécifiques pour chaque utilisateur ou groupe d'utilisateurs Active Directory. Ter Beke distingue trois niveaux d'autorité. Le cas échéant, il est également possible d'autoriser (ou d'exclure) des sites ou des catégories de sites spécifiques pour chaque adresse IP ou utilisateur. Si une personne se voit attribuer une nouvelle fonction, il suffit de lui allouer dans Active Directory les permissions correspondant à son nouveau groupe, et le pare-feu modifie automatiquement l'accès en conséquence. « C'est la même chose dans tous les pays, » précise Jorgen De Wael. « Qu'une personne se connecte depuis l'étranger ou durant un déplacement via un VPN, les règles sont appliquées partout en fonction de son profil dans l'annuaire Active Directory de Waarschoot. Les mêmes règles et les mêmes groupes sont utilisés localement avec les plus modestes appliances XTM. Lors des pics d'utilisation, il n'est pas rare de voir simultanément plus de 400 sessions utilisateur clients lourds et légers. »

Les utilisateurs bénéficient du même accès quel que soit l'endroit

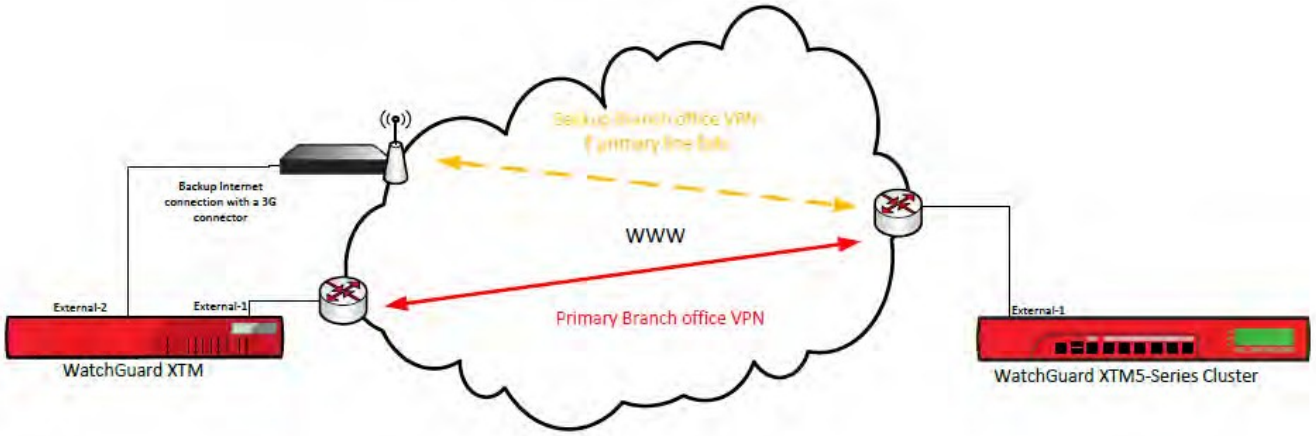


La direction informatique et la DRH déterminent ensemble ce que les utilisateurs peuvent et ne peuvent pas faire au-delà du niveau d'autorisation correspondant à leur fonction. « En ce qui concerne les applications, actuellement nous nous contentons de définir celles qui peuvent être utilisées au sein du proxy http(s). Par exemple, supposons que certains membres de notre service marketing soient autorisés à utiliser Facebook. Si nous le souhaitons, nous pouvons alors définir qu'au sein de cette application, ils peuvent discuter mais ne peuvent pas jouer à des jeux. »



	Application	Hits
+	Microsoft Internet Explorer	141,766
+	DNS	73,778
+	SSL/TLS	40,795
+	HTTP	28,710
+	World Wide Web HTTP	26,486
+	SMTP	21,962
+	FTP Applications	18,063
+	Android browser	7,142
+	Mozilla Firefox	4,132

Parce que la disponibilité est extrêmement importante, Ter Beke assure la redondance au niveau du pare-feu mais a également opté pour des liaisons redondantes sur les sites distants. Lorsque c'est possible, une liaison physique de backup est donc utilisée via un « second » fournisseur. Certains sites sont en fait très lointains et il n'est donc pas toujours possible d'obtenir une seconde liaison physique Internet via un autre fournisseur. C'est pourquoi, pour ses sites distants, Ter Beke s'appuie sur le Broadband Extend Wireless Bridge de WatchGuard, qui fournit une connexion Internet de secours basée sur un réseau 3G.



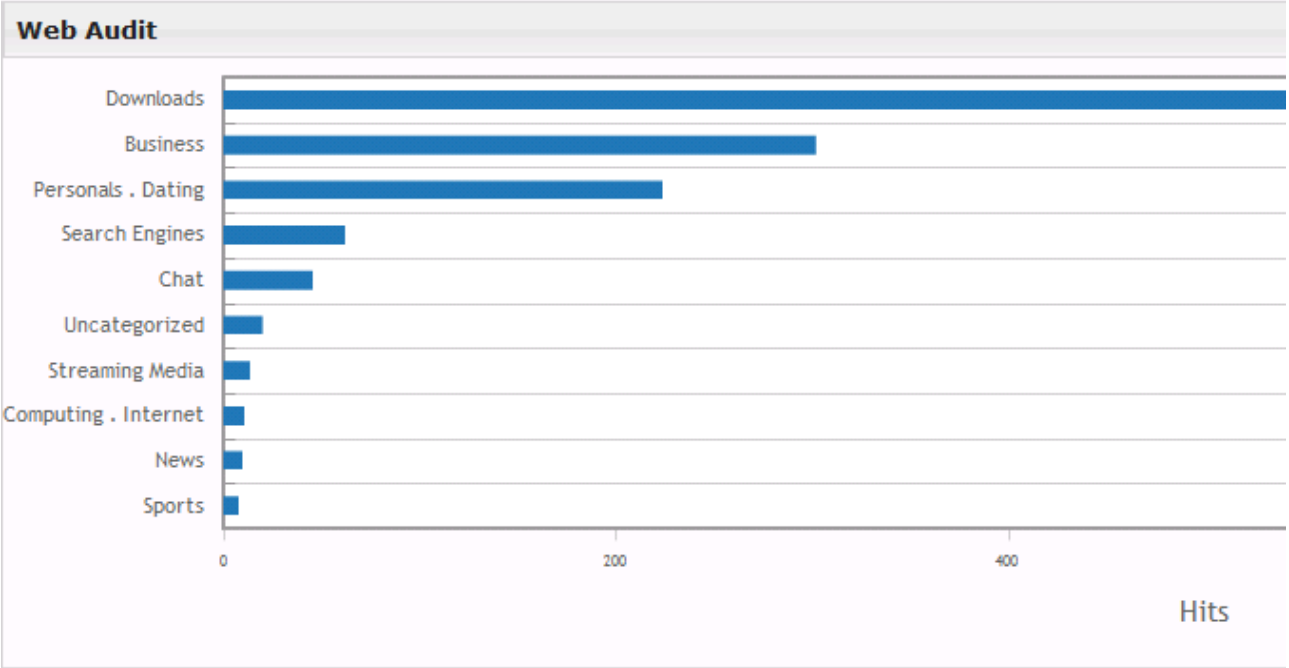
Basculement Internet vers le 3G mobile

Economies et convivialité

Une fois le processus de transformation achevé, Marc Decroos a constaté une bien meilleure visibilité sur l'utilisation de la bande passante. « C'est là tout le secret. Les outils ne sont pas destinés à surveiller nos collègues. Je souhaite juste savoir ce qui est utilisé dans chaque application. »

La solution WatchGuard utilisée par Ter Beke comprend le bundle UTM qui assure une protection efficace contre tout type de menace : outre le filtrage d'URL, il comprend également de nombreuses fonctionnalités de protection (IPS, contrôle d'application, antispam, antivirus de passerelle et autorité de réputation).

« Nous avons bénéficié d'économies réellement significatives grâce à cette consolidation, » constate avec satisfaction Marc Decroos. « La solution antispam de notre fournisseur WAN, facturée sous la forme d'un abonnement mensuel pour chaque utilisateur, nous coûtait très cher chaque mois, notre solution antivirus exigeait un serveur dédié et le filtrage d'URL représentait aussi un abonnement relativement coûteux. Les économies obtenues rien que sur l'antispam et le filtrage d'URL pour 500 utilisateurs concurrents représentent près de 10 000 euros par an. Suite à la consolidation, deux serveurs Microsoft se sont également avérés superflus. Nous avons supprimé tous les coûts possibles. Nous sommes en outre désormais capables d'offrir à nos utilisateurs une expérience de travail bien plus conviviale. Mon collègue Jorgen De Wael a eu la joie de pouvoir supprimer les exceptions accumulées sur le serveur ISA, et grâce aux rapports WatchGuard, il a désormais la possibilité de savoir en permanence ce qui se passe réellement sur son réseau. Le fait que WatchGuard s'avère aussi efficace dans la protection de notre environnement Citrix et de serveurs terminaux a incontestablement constitué pour notre projet la cerise sur le gâteau. »



A PROPOS DE WATCHGUARD

Depuis 1996, WatchGuard Technologies fournit des appliances de sécurité fiables et simples à gérer à des centaines de milliers d'entreprises dans le monde. Les solutions de sécurité réseau WatchGuard XTM, plusieurs fois récompensées, associent des services VPN, de pare-feu et une suite de services de sécurité qui renforcent la protection dans les domaines d'attaque critiques. La ligne de produits XCS garantit la sécurité des contenus sur les messageries et le Web, ainsi que la prévention des pertes de données. Ces deux lignes de produits vous aident à atteindre vos objectifs de conformité réglementaire et sont proposées au choix sous forme d'appliances physiques ou d'éditions virtuelles. Représenté par plus de 15 000 partenaires répartis dans 120 pays, WatchGuard a implanté son siège à Seattle, dans l'état de Washington, et compte de nombreux bureaux en Amérique du Nord, en Amérique Latine, en Europe et dans la zone Asie-Pacifique. Pour en savoir plus, visitez www.watchguard.fr

WatchGuard France : 01 47 90 30 35 ou france@watchguard.com