Reprenez le contrôle : Gérer les applications non productives, inappropriées ou dangereuses devient indispensable

Livre blanc sur le contrôle d'application

WatchGuard® Technologies, Inc.
Juin 2011

Introduction : concilier productivité et sécurité

Les employés trouvant de nouvelles manières « créatives » d'utiliser le Web, les entreprises s'efforcent de maintenir le contrôle de leur réseau tout en permettant à leurs salariés, partenaires ou autres acteurs d'accéder aux fonctionnalités essentielles. De nouvelles applications sont apparues en nombre et ne cessent de croître chaque jour. Un fait complique la situation : ce qui caractérise une « bonne » et une « mauvaise » application n'est plus nettement défini. Certaines applications ont un objectif purement professionnel et sont conçues avec soin afin de réduire les risques de sécurité et d'optimiser la productivité. À l'autre extrémité de la série de risques se trouvent les applications programmées pour voler des données, corrompre les ordinateurs et interrompre l'activité réseau. Une grande diversité d'applications se trouve entre ces deux extrêmes.

L'évolution des applications complique la sécurité

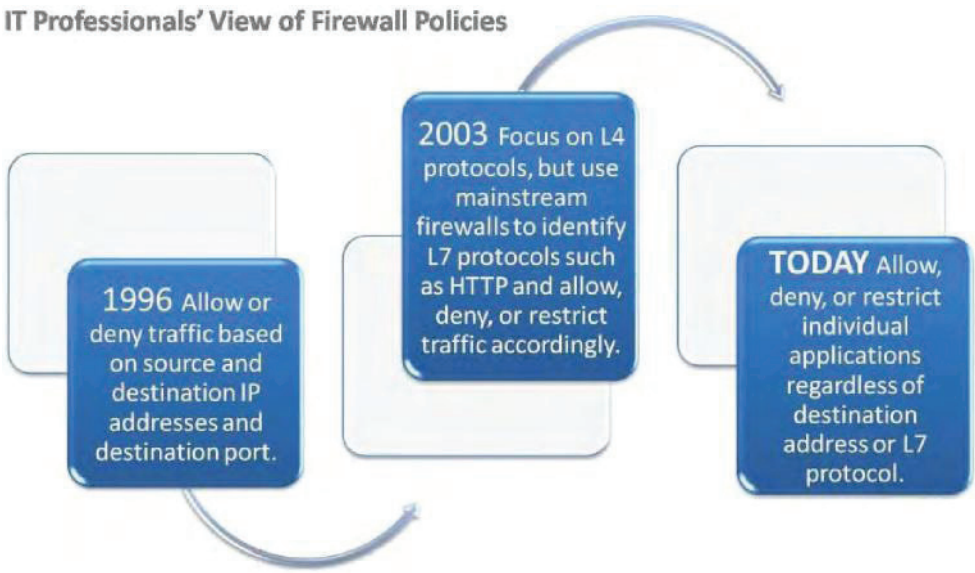
Les administrateurs informatiques étaient auparavant en mesure de refuser l'accès aux applications dont les origines appartenaient au monde du grand public, mais une telle stratégie s'avère à présent de plus en plus problématique. Après tout, les applications telles que Facebook se sont avérées assez fructueuses pour de nombreux professionnels, en particulier les groupes commerciaux et marketing.
En fait, 1,5 million d'entreprises locales possèdent des pages actives sur Facebook. (Pour plus d'informations à ce sujet et sur d'autres sujets intéressants concernant Facebook, consultez la page:
http://www.digitalbuzzblog.com/facebook-statistics-facts-figures-for-2010/).
En parallèle, les jeux Facebook peuvent nuire à la productivité et présentent également un risque de sécurité s'ils contiennent du code malveillant).

Cette évolution pousse les administrateurs à réévaluer leur configuration des pare-feux permettant de protéger l'environnement d'entreprise. Il y a quelques années, les administrateurs pouvaient refuser l'accès aux applications en instaurant des politiques de pare-feux bloquant certains ports ou protocoles. De nombreuses applications apparaissant maintenant comme du trafic Web sur les ports 80 ou 443, cette méthode n'est plus suffisante ni efficace. Ainsi, une part importante du contrôle sur les applications utilisées au sein de l'entreprise n'est plus possible sans de nouvelles technologies.

Des niveaux de contrôle de nouvelle génération sont nécessaires et les applications de messagerie instantanée (IM, Instant Messaging) et de peer-to-peer (P2P) constituent des exemples frappants de cette nécessité.
La première génération d'applications de ce type aurait pu être maîtrisée via des listes de contrôle d'accès (ACL) basiques axées sur des ports de destination fixes ou limités et des serveurs d'enregistrement facilement identifiables.
Les applications de seconde génération utilisaient des ports et serveurs d'enregistrement dynamiques qui changeaient souvent d'adresse ou qui étaient mis en miroir de manière intensive afin de diminuer l'efficacité des ACL pour bloquer les applications. Les applications IM et P2P actuelles agissent souvent comme du trafic Web et, dans de nombreux cas, rendent les serveurs d'enregistrement complètement inutiles. Ainsi, elles sont de plus en plus en mesure de détourner les pare-feux. En fait, certaines applications, notamment Ultrasurf et Skype, échappent aux technologies de sécurité à dessein. Les entreprises ont clairement besoin de contrôler étroitement l'accès à de telles applications, en particulier les entreprises tenues par des normes en vigueur dans certains secteurs.

Les administrateurs informatiques doivent reprendre le contrôle

L'historique ci-dessous illustre les fonctionnalités recherchées par les professionnels de la sécurité dans une solution.



Pour sécuriser les environnements d'entreprise actuels et reprendre le contrôle, les administrateurs doivent identifier et déterminer si les applications sont utilisées à des fins professionnelles légitimes, si elles représentent du code malveillant ou si elles se situent entre ces deux extrêmes. Dans ce dernier cas, les professionnels de l'informatique doivent être en mesure de contrôler quelles personnes peuvent accéder à ces applications et à quelles fins. Les applications Web 2.0 telles que la diffusion de fichiers multimédia et audio peuvent consommer de grandes quantités de bande passante onéreuse. En outre, les entreprises opérant dans des secteurs réglementés peuvent devoir restreindre l'utilisation de la messagerie instantanée car elles ne peuvent sinon se conformer aux exigences de rétention des messages électroniques. Dans le cadre de mesures de conformité en termes de sécurité et de réglementation, d'une politique d'entreprise d'usage conforme ou d'une combinaison de ces dernières, les entreprises doivent contrôler comment les employés utilisent une large gamme d'applications.

Les risques de sécurité engendrés par les applications

Le Web constitue la principale source de menaces pour la sécurité auxquelles font face les entreprises modernes et les applications Web représentent souvent la première cible des pirates. En même temps, les réseaux sociaux évoluent rapidement et de nouveaux sites Web 2.0 naissent çà et là. Les utilisateurs doutent encore souvent de la manière dont s'exercent les niveaux adéquats de confidentialité sur de tels sites. Ainsi, les pirates jugent pratique d'exploiter les réseaux sociaux comme point de départ à leurs attaques d'ingénierie sociale ciblant les employés d'une entreprise. Les utilisateurs ont tendance à se fier davantage aux liens vers des sites partagés par une personne de leur réseau social sans réaliser que de tels comptes peuvent être usurpés ou faux.
Étant donné que le trafic et les applications Web constituent la source de nombreux risques de sécurité, les administrateurs informatiques peuvent réduire les vecteurs de menaces potentiels en limitant leurs utilisateurs aux seules applications nécessaires d'un point de vue professionnel.

WatchGuard Application Control

WatchGuard optimise en permanence ses solutions pour suivre le rythme des défis les plus récents auxquels sont confrontées les entreprises de toutes tailles. L'appliance WatchGuard XTM v11.4 (et les versions ultérieures) comprennent des fonctionnalités de contrôle applicatif permettant aux administrateurs d'exercer un contrôle fin sur des centaines d'applications et de déterminer quelles applications sont utilisées et par qui.

WatchGuard Application Control constitue une solution de sécurité par abonnement entièrement intégrée disponible pour toutes les appliances WatchGuard XTM. Cette solution offre une supervision et un blocage globaux et basés sur des politiques de plus de 1 800 applications Web et commerciales différentes, pour une productivité accrue et une sécurité renforcée.
Les administrateurs peuvent appliquer les politiques d'usage conformes pour les utilisateurs et groupes selon une catégorie, une application et une sous-fonction d'application. Par exemple, ils peuvent instaurer une politique autorisant le service marketing à accéder à Facebook, mais ne l'autorisant pas à accéder aux jeux Facebook.

Les dangers du World Wide Web

40 000 sites Web sont compromis chaque semaine et 0,7 % des résultats de recherche Google affichent des sites infectés par du code malveillant. Source : Google Security Blog, 25 août 2009.

Les attaques visant les applications Web représentent plus de 60 % de l'ensemble des tentatives d'attaque observées sur Internet. Source : SANS Top 10 Security Risks (Les 10 risques majeurs de sécurité selon le SANS), septembre 2009.

64 % des personnes interrogées par AVG ont cliqué sur des liens fournis par des membres de communauté de réseaux sociaux et 26 % ont partagé des fichiers au sein de réseaux sociaux. Source : AVG, Social Engineering: Hacking people, not machines (Ingénierie sociale : pirater des personnes et non des machines), 2009.

Exploitant plus de 2 500 signatures et techniques de comportement avancées, Application Control dote également l'administrateur d'une visibilité historique et en temps réel de l'utilisation (ou des tentatives d'utilisation) des applications sur le réseau. Ce niveau de contrôle et de visibilité aide les entreprises à instaurer des politiques d'usage conforme exigées par les normes en vigueur dans certains secteurs, les autorités juridiques et politiques, les objectifs ou la culture de l'entreprise et autres.

Mode de fonctionnement de WatchGuard Application Control

Dans l'outil de configuration WatchGuard XTM, l'administrateur met en œuvre une politique globale ou plus granulaire concernant des utilisateurs, groupes ou réseaux spécifiques, ou selon d'autres critères déterminant les applications pouvant être utilisées ou non. WatchGuard XTM Application Control inspecte ensuite en temps réel le trafic transitant par l'appliance et détermine quelles applications en sont à l'origine. Une technologie basée sur les signatures, combinée à un moteur évaluant le comportement applicatif permet à l'appliace d'identifier les applications avec un degré élevé de précision. L'appliance met en œuvre la politique définie par l'administrateur et consigne ses actions à des fins d'analyse. L'administrateur peut se connecter à l'interface graphique de reporting pour consulter l'usage de l'application, par exemple quelles applications les utilisateurs exécutent (ou tentent d'exécuter) et celles les plus employées dans l'ensemble de l'entreprise.

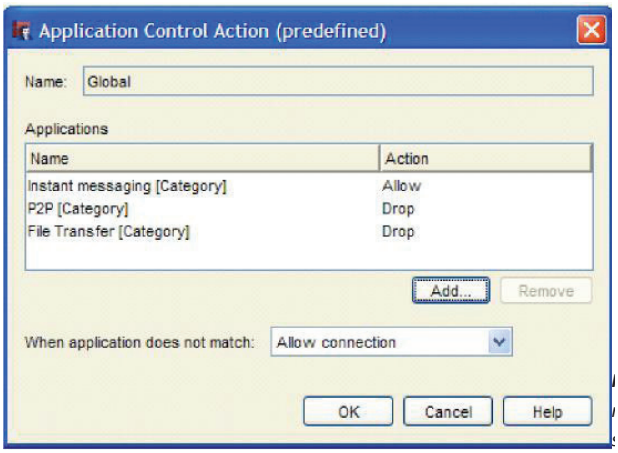


Figure 1. *Les administrateurs peuvent facilement maintenir des paramètres de politiques globales sur le réseau d'entreprise.*

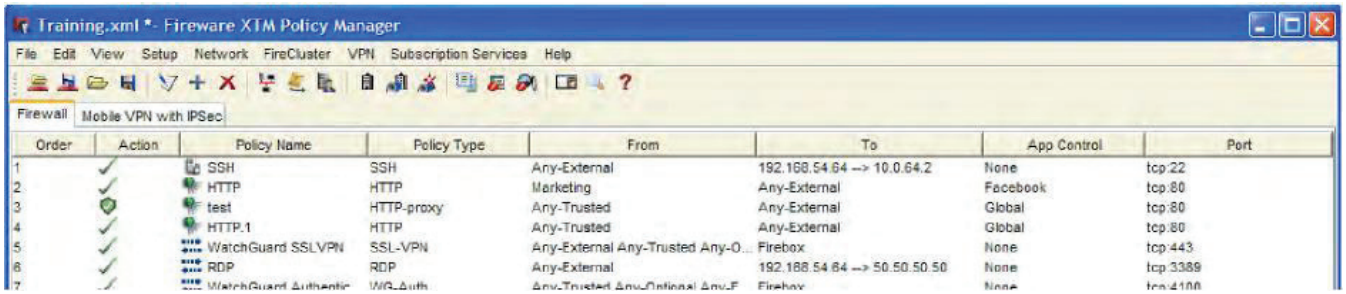


Figure 2. *L'administrateur peut exercer un contrôle fin sur des centaines d'applications, organisées selon leurs catégories, et peut également contrôler quelles personnes utilisent quelles applications et à quels moments.*

Grâce à WatchGuard Application Control, les entreprises peuvent exercer un contrôle granulaire sur l'utilisation des applications sur le réseau d'entreprise. Elles peuvent par exemple :

- Bloquer l'utilisation de YouTube, Skype et QQ.
- Bloquer l'utilisation de toutes les applications P2P pour les utilisateurs n'appartenant pas à l'équipe de direction.
- Autoriser l'accès à des sites de réseaux sociaux tels que Facebook et Twitter au service marketing.
- Autoriser l'utilisation de Windows Live Messenger pour la messagerie instantanée, mais ne pas autoriser le transfert de fichiers via Windows Live Messenger.
- Limiter l'utilisation des applications de diffusion multi média à des heures spécifiques.
- Analyser les 10 applications les plus utilisées dans l'entreprise.
- Analyser l'utilisation (ou les tentatives d'utilisation) des applications par chaque personne au sein de l'entreprise.

Les applications Web : multiples et variées

Messageries instantanées
QQ, Windows Live Messenger, Yahoo!

E-mail
Hotmail, Gmail, Yahoo, Microsoft

Web 2.0 :
Facebook, LinkedIn, Twitter, Salesforce

Peer to Peer
Gnutella, Foxy, Winny, BitTorrent, eMule

Serveurs d'accès à distance
TeamViewer, GoToMyPC, Webex

Bases de données
Microsoft SQL, Oracle

Transfert de fichiers
Peercast, Megaupload

Voice over IP
Skype

Diffusion multimédia
QuickTime, YouTube, Hulu

Gestion réseau
Microsoft Update, Adobe, Norton,

Tunnel (proxys de contournement Web)
Avoidr, Ultrasurf, Circumventor

Que rechercher dans une solution de contrôle applicatif ?

Lorsqu'il s'agit de choisir une solution de contrôle applicatif, il s'avère essentiel de rechercher les critères suivants :

- **Contrôle granulaire.** contrôlez un ou plusieurs aspects d'une application tout en étant en mesure de rejeter d'autres as pects de celle-ci afin de s'adapter aux divers modes d'utilisation des applications. Vous pouvez par exemple autoriser l'utilisation de Windows Live Messenger pour la messagerie instantanée mais pas pour le transfert de fichiers ou autoriser l'accès à Facebook mais pas pour les jeux Facebook.

- **Richesse des signatures d'application.** Recherchez une liste tendue de signatures mises à jour et maintenues sur le long terme par le fournis seur. Dans l'idéal, à mesure que de nou velles applications sont lancées et que les comportements applicatifs évoluent, les signaturesdevraient être automatiquement actualisées sans nécessiter de mise à niveau de l'ensemble d'une application de sécurité.

- **Identification des applications chiffrées.** Les ingénieurs logiciels experts tentent de contourner les mesures de sécurité en chiffrant les données applicatives et le trafic Internet. La meilleure solution consiste à exploiter l'analyse comportementale pour découvrir les applications même les plus masquées.

- **Intégration à l'ensemble des politiques.** Il n'est pas suffisant d'utiliser des fonctionnalités complémentaires dans un service de prévention d'intrusion pour s'adapter à quelques applications. Cherchez une solution permettant l'instauration de contrôles applicatifs dans le cadre de politiques de pare-feu basiques.

- **Équilibre entre performances et efficacité.** Certains produits qui proposent un contrôle applicatif nécessitent un matériel coûteux pour offrir des niveaux de performances acceptables. Les entreprises doivent s'assurer que leurs produits de sécurité offrent de hautes performances à un coût raisonnable ainsi que l'efficacité du contrôle applicatif qu'exigent ces derniers.

Avantages pour les administrateurs informatiques et l'entreprise

En exploitant Application Control de WatchGuard, les entreprises vont bénéficier de nombreux avantages. Outre une reprise du contrôle sur l'environnement d'entreprise, les administrateurs informatiques exercent en fait plus de pouvoir sur les applications que par le passé. Ils peuvent ainsi suivre le rythme de l'environnement applicatif en constante évolution et répondre aux demandes de l'entreprise et des utilisateurs. En fait, en appliquant des politiques contrôlant l'usage des applications, les administrateurs s'assurent que les employés et autres utilisateurs peuvent travailler comme ils en ont besoin, qu'ils restent concentrés et productifs et qu'ils évitent les éventuels problèmes juridiques liés à l'utilisation d'applications non autorisées. Tout aussi important : en mettant en œuvre un contrôle applicatif complet, les entreprises peuvent s'assurer de limiter leurs risques de sécurité et de préserver la bande passante pour des applications et une utilisation cohérentes avec les objectifs métier.

WatchGuard XTM : un pare-feu complet pour le contrôle applicatif

Les employés, partenaires et autres acteurs de l'environnement d'entreprise bénéficiant d'un accès simple à une vaste gamme d'applications, les entreprises doivent déterminer une manière de concilier les besoins de leurs utilisateurs avec la sécurité. Alors que de nombreuses applications vont à l'encontre d'une simple catégorisation, les administrateurs informatiques nécessitent de nouveaux degrés de contrôle sur les applications et les utilisateurs autorisés.

Ce type de contrôle applicatif est disponible à présent dans le pare-feu de WatchGuard XTM. WatchGuard le propose dans le cadre d'un pare-feu complet comprenant toutes les fonctionnalités nécessaires pour sécuriser de manière simple, complète et rentable l'environnement d'entreprise. Outre l'élaboration et l'application de politiques avancées axées sur les applications, XTM prend en charge toutes les configurations classiques basées sur des ports et protocoles que connaissent les administrateurs, ainsi que des fonctionnalités réseau essentielles, notamment le routage dynamique, le basculement de WAN et la répartition de charge. Une méthode de VPN par glisser-déposer facilite la création de canaux site-à-site pour des connexions sécurisées entre les lieux. En outre, une suite d'outils de supervision en temps réel et interactifs permet de gagner du temps et d'observer en un coup d'œil les informations sur les utilisateurs, le réseau et les activités de sécurité.

En plus d'un rapport performances/prix leader sur le marché, WatchGuard XTM propose plusieurs autres solutions de sécurité par abonnement offrant des fonctionnalités complètes de gestion des menaces :

- **Reputation Enabled Defense :** Offre un service de réputation d'URL efficace sur le cloud protégeant les utilisateurs Web contre les pages contenant du code malveillant, tout en optimisant de manière significative le débit Web.

- **spamBlocker :** Bloque les messages indésirables avec une précision proche de 100 % ainsi que les charges utiles virales souvent engendrées par le spam. spamBlocker reconnaît le spam quel que soit le langage, format ou contenu du message, même le spam basé sur des images que les autres produits antispam ne détectent souvent pas.

- **WebBlocker :** Service de filtrage d'URL bloquant l'accès aux sites Web dangereux ou inappropriés sur le lieu de travail. Il filtre les URL sur HTTP et HTTPS afin de combler les lacunes du protocole HTTPS souvent négligées par de nombreux autres filtres Web.

- **Antivirus de passerelle :** Offre une protection éprouvée basée sur les signatures au niveau de la passerelle contre les virus, chevaux de Troie, vers, logiciels espions et logiciels rogues connus.

- **Prévention d'intrusion :** Analyse tous les ports et protocoles pour bloquer les attaques conformes aux protocoles standard mais contenant du code malveillant, notamment des débordements de tampon, l'injection de code SQL et les intégrations de fichiers à distance.

Pour en savoir plus sur WatchGuard Application Control et la gamme d'appliances de sécurité réseau XTM, contactez-nous au 03 81 88 54 54

ADRESSE :

505 Fifth Avenue South
Suite 500
Seattle, WA 98104

SITE WEB :
www.watchguard.com

VENTES ÉTATS-UNIS :
1.800.734.9905

VENTES INTERNATIONALES :
+1.206.613.0895

À PROPOS DE WATCHGUARD

Depuis 1996, WatchGuard Technologies offre des appliances de sécurité fiables et faciles à gérer à des centaines de milliers d'entreprises dans le monde entier. Les solutions de sécurité réseau primées de Watchguard, notamment les solutions gestion évolutive des menaces (XTM), combinent pare-feux, VPN et services de sécurité. Les appliances de sécurité évolutive du contenu (XCS) offrent une sécurité du contenu de messagerie et Web, ainsi qu'une prévention des pertes de données. Ces deux gammes de produits vous aident à répondre aux exigences en termes de conformité réglementaire, notamment PCI DSS, HIPAA, SOX et GLBA. Plus de 15 000 partenaires représentent WatchGuard dans 120 pays. WatchGuard, dont le siège se trouve à Seattle et Washington (États-Unis), possède des bureaux couvrant l'Amérique du Nord, l'Europe et l'Amérique latine. Pour plus d'informations, consultez le site www.watchguard.fr