



コントロールを取り戻そう： セキュリティ強化＋社員に権限＋ ビジネスも守る

アプリケーションコントロール(ホワイト・ペーパー)

2010年10月

はじめに:セキュリティで生産力にバランスを

社員が新しくクリエイティブな方法でウェブを利用する方法を見つけるに連れ、組織は重要機能へのアクセス権を所持している社員やパートナー、関係者などに権利を委託しつつ、企業ネットワークのコントロールを維持していくのに四苦八苦している。膨大な数の新しいアプリケーションが出回っており、その数は日々増加している。アプリケーションの善し悪しを定める点やその違いは、これまでのように明快な問題ではなくなっているため問題をより複雑にしている。アプリケーションの中には、ビジネスを目的としセキュリティ・リスクを最低限に抑え、生産力を最大限に引き伸ばすものもある。そしてその一方では、データを盗みコンピュータを破壊し、ネットワーク・アクティビティを中断させるようにプログラムされているアプリケーションもある。また、実に様々なアプリケーションは、そうした両極端の中間に位置している。

セキュリティを複雑にするアプリケーションの進化

IT管理者は消費社会を基盤にしたアプリケーションを拒否する傾向にあったが、そうしたアプローチは次第に問題になってきた。それというのは、やはりFacebookのようなアプリケーションはビジネス社会、特にセールス・グループやマーケティング・グループにおいても非常に有益であることが証明されており、実際Facebookにページを設けているローカル・ビジネス数は150万にも上っている(Facebookに関する興味深い事実については、こちらの記事を参照：<http://www.digitalbuzzblog.com/facebook-statistics-facts-figures-for-2010/>)。しかし、それと同時にFacebookのゲームは生産力を大きく妨げ、ゲームにマルウェアが入っていた場合はセキュリティ・リスクにもつながる。

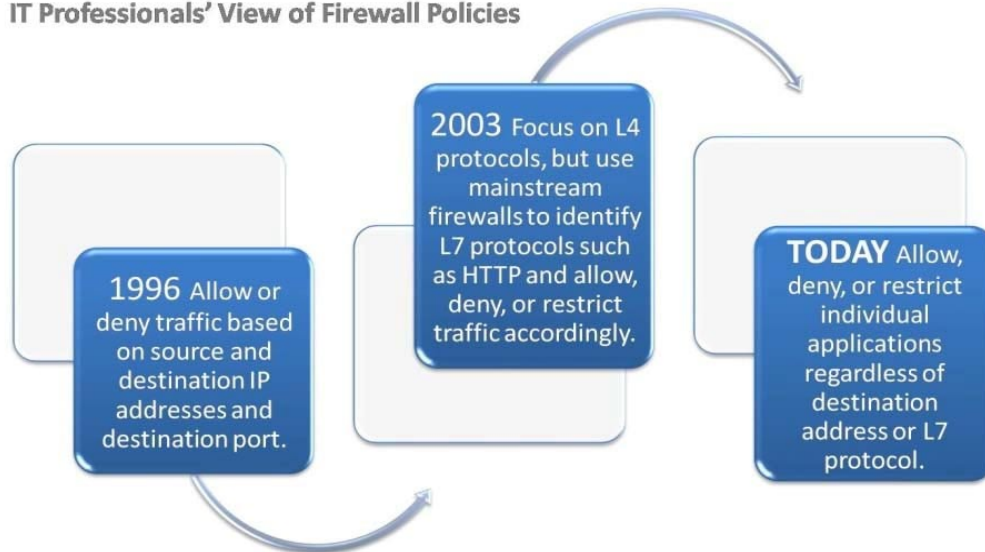
アプリケーションの進化は企業環境を保護する上で、管理者達がファイアウォールをいかに設定すべきか見直さなければならぬ原因になっている。数年前であれば、IT管理者が特定のポートやプロトコルをブロックすることでファイアウォール・ポリシーを定義し、アプリケーションへのアクセスを拒否することができた。しかし、最近のアプリケーションの多くはポート80やポート443のウェブ・トラフィックとして現れるため、そういったアプローチでは事足りなく、効果的ではない。結果として、管理者は企業ネットワークで使用されているアプリケーションをコントロールする権利を大幅に失うことになってしまったのだ。

新しいレベルのコントロールの必要性を表す典型的な例としては、インスタント・メッセージ(IM)やピアツーピア(P2P)アプリケーションがある。IMやP2Pアプリケーションの第一世代は、固定またはデスティネーション・ポートや敏速に認識するレジストレーション・サーバなどに基いたベーシックなアクセス・コントロール・リスト(ACL)で規制することができた。第二世代アプリケーションは、アプリケーション・ブロック機能の効果が低いACLを無効にするため、頻繁にアドレス変更を行ったりミラーするダイナミック・ポートやレジストレーション・サーバを広範囲に渡り使用した。そして、最近のIMやP2Pアプリケーションでは、ウェブ・トラフィックのように移動するケースが多く見られ、大方の場合レジストレーション・サーバを省略しているため、結果としてファイアウォールを巧妙に回避することができるようになっている。実のところ、Ultrasurfやスカイプ、ウィニーといったアプリケーションは意図的かつ巧妙にセキュリティ技術を回避することができるため、企業はそうしたアプリケーションへのアクセスを細かにコントロールしなければならない必要があるのは明らかだ。特定の業界規制を受けている組織は特に注意したい点である。

IT管理者達を取り戻すべきコントロール

下記のタイムラインは、現状のセキュリティ・プロフェッショナルがソリューションに求める機能を図で表している。

IT Professionals' View of Firewall Policies



管理者達が現状の企業環境を安全にし、そのコントロールを取り戻すためには、正当なビジネス目的で使われているアプリケーションがマルウェアなのか、それとも中間に落ち着くタイプなのかを確認し判断しなければならない。後者の場合、ITプロフェッショナルは、そのアプリケーションに誰が何の目的でそれにアクセスできるかコントロールする必要がある。メディアやオーディオ・ストリーミングなどのWeb 2.0アプリケーションは、高額な企業バンド幅を大量に消耗する。更に、規制のある業界の企業らは、電子メッセージ保持規制に準拠できないためインスタント・メッセージングの利用を制限しなければならないかもしれない。セキュリティの一部として、また企画順守の一部として、企業の許容範囲内の利用規定またはその2つの組み合わせにおいて組織は社員のアプリケーション使用を完全にコントロールする必要がある。

アプリケーションに伴うセキュリティ・リスク

現状の組織に対する主なセキュリティ脅威はウェブで、攻撃者達の主な焦点はウェブ・アプリケーションである。それと同時にソーシャル・ネットワークは急速に成長を遂げており、新しいWeb 2.0サイトは次から次へと出現している。しかし、ユーザはそうしたサイトにおいて、どういったプライバシー・レベルを使えば適切であるのか不確かなケースがまだ多く、結果としてハッカーは社員に対して仕掛けるソーシャル・エンジニアリング攻撃の拠点にソーシャル・ネットワークを使うことが便利だと見ている。ユーザは、ソーシャル・ネットワークつながりの相手からサイトのリンクを受取っても、そのアカウントがスプーフィングされていたり、偽りのものであることに気付かず、そのリンクを信頼しやすい傾向がある。

多数のセキュリティ・リスクの原因であるウェブ・トラフィックやウェブ・アプリケーションをユーザが使用せず、ビジネス目的に必要なアプリケーションのみを使うように許可することで、こうした脅威の可能性を軽減することができる。

WatchGuard Application Control

ウォッチガードのソリューションは組織の規模にかかわらず、新たなチャレンジに対応できるように進化し続けている。WatchGuard XTMアプライアンスv11.4(およびそれ以降のバージョン)には、管理者が何百ものアプリケーションを細かにコントロールすることを可能にし、どのアプリケーションが誰によって使われているのかが分かるアプリケーションコントロール機能が搭載されている。

WatchGuard Application Control は、WatchGuard XTMアプライアンスすべてのセキュリティ・サブスクリプションに完全統合されている。この機能は1,500以上の固有のウェブやビジネス・アプリケーションに対し、グローバルおよびポリシーベースの監視やブロックを行い、より優れた生産力とセキュリティ強化を提供している。管理者達は、カテゴリ、アプリケーション、アプリケーションのサブ機能別などで、ユーザやグループに対し許容範囲内の使用規制を強化することができる。例えば管理者達は、マーケティング部がFacebookにアクセスすることができても、Facebookのゲームにはアクセスできないようにポリシーを規定することができる。

アプリケーションコントロールは 2,300以上のシグネチャとアドバンス行動法を使い、ネットワークにおけるアプリケーション使用の履歴を(使用を試みたものも含む)管理者がリアルタイムで見られるようにする。そうしたレベルのコントロールや、ネットワークを見渡せる力は業界規制や法律、行政区、企業目標や文化などにより命じられている組織の許容範囲内ポリシーの強化に役立つ。

WatchGuard Application Control の機能

WatchGuard XTMコンフィギュレーション・ツールでは、管理者がグローバル・ポリシーを設定したり、より細かに特定のユーザやグループ、ネットワークを対象とした設定、またはその他の基準を使うことで、ユーザがどのアプリケーションを使用でき、できないかを定めることができる。アプリケーションコントロールを使うWatchGuard XTMは、アプライアンスにアプローチするトラフィックをリアルタイムで検査し、どのアプリケーションがそのトラフィックを生成しているのか判断できる。アプリケーションの行動を査定するエンジンと組み合わせたシグネチャ・ベース技術は、アプライアンスが高い正確度でアプリケーションを識別することができる。アプライアンスは管理者が規定したポリシーを強化し、再調査の時のために、そのアクションを記録することもできる。どのアプリケーションをユーザが実行しているか、ビジネスではどのアプリケーションが頻繁に使われているのかなど、管理者はレポートされるGUIにログインしアプリケーションの使用量を見ることができる。

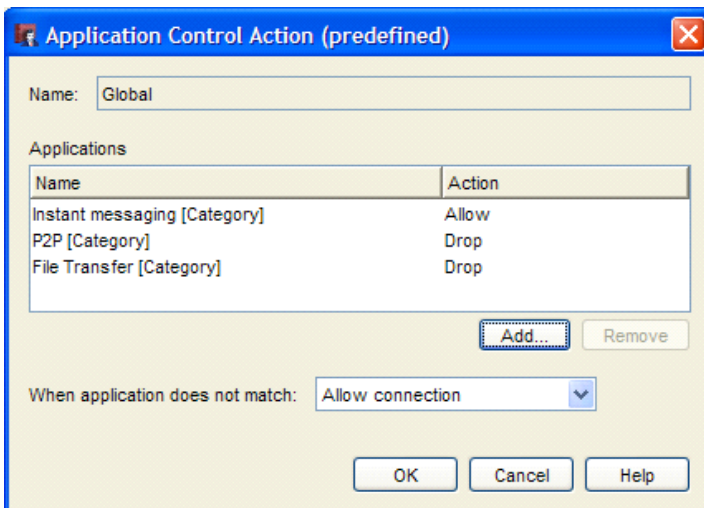


図1. 管理者達はグローバル・ポリシー設定を企業ネットワークで簡単に管理できる。

インターネットの危険性

障害のあるウェブサイト数は毎週4万件もあり、グーグル検索結果の0.7%はマルウェア感染を受けているサイトを表示している。

情報源: 2009年8月25日 -

[グーグル・セキュリティ・ブログ](#)より

インターネットで観察された攻撃全体の60%以上は、ウェブ・アプリケーションに対する攻撃だった。

情報源: 2009年9月 -

[SANSトップ10セキュリティ・リスク](#)より

AVG調査対象の64%は、ソーシャル・ネットワーク繋がりのメンバーから受取ったリンクをクリックするという。又、26%はソーシャル・ネットワーク内でファイルをシェアしているという。

情報源: 2009年

AVG, Social Engineering: Hacking people, not machinesより

Order	Action	Policy Name	Policy Type	From	To	App Control	Port
1	✓	SSH	SSH	Any-External	192.168.54.64 --> 10.0.64.2	None	tcp:22
2	✓	HTTP	HTTP	Marketing	Any-External	Facebook	tcp:80
3	✓	test	HTTP-proxy	Any-Trusted	Any-External	Global	tcp:80
4	✓	HTTP.1	HTTP	Any-Trusted	Any-External	Global	tcp:80
5	✓	WatchGuard SSLVPN	SSL-VPN	Any-External Any-Trusted Any-O...	Firebox	None	tcp:443
6	✓	RDP	RDP	Any-External	192.168.54.64 --> 50.50.50.50	None	tcp:3389
7	✓	WatchGuard Authentic	W/G Auth	Any-Trusted Any-Optional Any-F	Firebox	None	tcp:4100

図2. 管理者は誰がどのアプリケーションをいつ使用するか、カテゴリ別に何百ものアプリケーションを細かにコントロールできる。

WatchGuard Application Control を使えば、企業ネットワークにあるアプリケーションの使用を細かに管理することが可能になる。

例えば:

- YouTubeやスカイプ、QQなどを使用禁止にできる
- マネージメント・チーム以外のユーザによるP2Pアプリケーションの使用を禁止できる
- FacebookやTwitterなどのソーシャル・ネットワーキングサイトにマーケティング部がアクセスできるように許可する
- インスタント・メッセージ用にWindows Liveメッセンジャーを許可しながら、Windows Liveメッセンジャーでのファイル転送を禁止できる
- ストリーミング・メディア・アプリケーションの使用許可時間を制限できる
- 企業内で使われているアプリケーションのトップ10の報告が可能
- 企業の個人ユーザが使用した(または使用を試みた)アプリケーションをレポートできる

アプリケーションコントロールに求めるもの

アプリケーションコントロール・ソリューションに求める点では次が重要な基準になる:

- **綿密なコントロール** 様々な方法でアプリケーションを使用するユーザ達に対応するには、アプリケーションのある面をコントロールしながら別の面を許可しないことが重要だ。例えばインスタント・メッセージを使うためにWindow Liveメッセンジャーを許可しているが、ファイル転送は禁止しているケース、Facebookへのアクセスは許可しているが、Facebookのゲームは許可していない、など。
- **広範なアプリケーション・シグネチャ** ベンダがこれまでにアップデートし、維持してきた広範なシグネチャ・リストを探せること。理想を言えば、新しいアプリケーションがリリースされ、アプリケーションの動きが変わったらセキュリティ・アプリケーション全体をアップグレードする必要なく、シグネチャが自動的にアップデートされること。
- **暗号化されたアプリケーションを識別できる力** 最近の抜け目ないアプリケーション・プログラマ達は、インターネットを移動するアプリケーション・データやトラフィックを暗号化することでセキュリティ対策を迂回しようとする。最良のソリューションは、行動分析を使うことで上手く偽装したアプリケーションさえも発見することができる。

遠く幅広くリーチできる ウェブベース・アプリケーション

インスタント・メッセージング

QQ, Windows Live Messenger, Yahoo! Messenger, GoogleTalk

電子メール

Hotmail, Gmail, Yahoo, Microsoft Exchange

Web 2.0

Facebook, LinkedIn, Twitter, Salesforce

ピアツーピア

Gnutella, Foxy, Winny, BitTorrent, eMule

リモート・アクセス・ターミナル

TeamViewer, GoToMyPC, Webex

データベース

Microsoft SQL, Oracle

ファイル転送

Peercast, Megaupload

VoIP

Skype

ストリーミング・メディア

QuickTime, YouTube, Hulu

ネットワーク・マネジメント

Microsoft Update, Adobe, Norton, McAfee, Syslog

トンネル(プロキシ迂回のウェブ)

Avoidr, Ultrasurf, Circumventor

- **ポリシーセットと合併** 侵入防止サービス内でアドオン機能を使うだけでは、複数のアプリケーション対応には充分ではないので、アプリケーションコントロールをベーシック・ファイアウォール・ポリシーの一部として設定できるソリューションを求めること。
- **効力を見せながらパフォーマンスのバランスを維持** アプリケーションコントロール機能を使うことができる製品には、満足できるレベルのパフォーマンスを提供する場合、高価なハードウェアを必要とするものもある。企業が使用するセキュリティ製品は高性能かつ手頃な価格で、必要なアプリケーション・コントロール機能の効力を出せるものでなければならない。

IT管理者とビジネスへの利点

WatchGuard Application Control を採用することで、組織は様々な利益を実現できる。企業環境のコントロール権を再び手にすることで、IT管理者達はこれまで以上にアプリケーションをコントロールできるようになる。結果的に、管理者達は進化し続けるアプリケーションの世界についていくことができるほか、企業やユーザの要求を満足させることもできる。実際、アプリケーション使用を管理するポリシー適用により、管理者達は社員やその他のユーザが必要な仕事をこなし集中力と生産力を確実に維持できるようにし、未認証のアプリケーション使用に伴う法律上の問題に遭遇する可能性も避けられるようにする。また、総合的なアプリケーションコントロールを使用することで、組織がセキュリティ・リスクを制限していることに疑いなく、企業のバンド幅をアプリケーション使用のために確保し、企業目標と一致したものであることを確実にすることも同様に重要な点である。

WatchGuard XTM: Application Control を可能にするフル機能ファイアウォール

企業環境内の社員やパートナーその他のユーザは、様々なアプリケーションにアクセスできるため、組織はユーザのニーズとセキュリティのバランスを図らなければならない。近頃のアプリケーションは明確にカテゴリ別にするのが困難なものが多いため、どのアプリケーションを許可し、誰がそれを利用できるかIT管理者達が決定するために必要な新しいレベルのコントロールが必要になっている。

このタイプのアプリケーションコントロールはWatchGuard XTMファイアウォールで使うことができる。ウォッチガードは簡単に総合的かつ費用効率がよく、安全な企業環境に必要な機能をすべて含むフル機能ファイアウォールの一部としてこの機能を提供している。XTMはアドバンス・アプリケーションベースのポリシー構築とその実施のほかにも、管理者達が慣れている従来のポートベースおよびプロトコルベースのコンフィギュレーション、ダイナミック・ルーティング、WANフェイルオーバー、ロードバランシングなど重要なネットワーク機能もサポートしている。また、ドラッグアンドドロップVPNの方法は、ロケーション間で安全な接続を設置するためのサイトツーサイト・トンネルを作成しやすくしている。更に、インタラクティブリアルタイム監視ツールは時間を節約し、ユーザやネットワーク、セキュリティ・アクティビティを一目で分かるようにしている。

更に、業界をリードする価格とパフォーマンスを提供するほか、WatchGuard XTMは総合的な脅威管理機能を実行するセキュリティ・サブスクリプションをいくつも提供している:

- **Reputation Enabled Defense:** パワフルなクラウドベースURLレピュテーション・サービスを提供。有害なウェブページからウェブ・ユーザを保護しながらダイナミックにウェブ・スループットを改善。
- **spamBlocker:** 不要メールをほぼ100%ブロックすることができる。スパムが大抵携えているウィルス性のペイロードもその対象になる。spamBlockerはメールで使われた言語やメール形式、その内容にかかわらずスパムを認識することができ、他のスパム対策製品が見落とすようなイメージベースのスパムさえも見分けることができる。
- **WebBlocker:** URLフィルタリング・サービスは、ビジネス環境にて危険かつ不適切なウェブサイトをブロックすることができる。WebBlockerはHTTPとHTTPSの両方でURLをフィルターに掛け、他のウェブ・フィルターがオープンにしたままである多くのHTTPSの抜け道を塞ぐことができる。
- **Gateway AntiVirus:** ゲートウェイにおいて、既知のウィルスやトロイの木馬、ワーム、スパイウェア、ログウェアに対しパワフルなシグネチャーベース保護を提供する。

- **Intrusion Prevention:** ポートやプロトコルをすべてスキャンし、スタンダード・プロトコルに準拠しているが、バッファ・オーバーフローやSQLインジェクション、リモートファイルなど有害なコンテンツを含む攻撃をブロックする。

WatchGuard Application Control や、ネットワーク・セキュリティ・アプライアンスのXTM製品シリーズの詳細については、WatchGuard認定リセラーにお問い合わせ下さい。また、弊社ウェブサイト<http://www.watchguard.co.jp/>からも連絡先や詳細をご覧ください。

住所:

505 Fifth Avenue South
Suite 500
Seattle, WA 98104

ウェブサイト:
www.watchguard.com

北米営業部:
1.800.734.9905

インターナショナル:
+1.206.613.0895

ウォッチガードについて

ウォッチガード・テクノロジー社は、1996年から信頼性が高く、管理しやすいセキュリティソリューションを世界中の何百、何千もの企業に提供しています。WatchGuardの受賞経験のあるエクステンシブル・スレット・マネージメント(XTM)ネットワーク・セキュリティソリューションは、ファイアウォールやVPN、セキュリティ・サービスを組み合わせたものです。エクステンシブル・コンテンツ・セキュリティ(XCS)アプライアンスは、メールやウェブ、データ紛失防止においてもコンテンツ・セキュリティを提供します。両製品シリーズはPCI DSS/HIPAA/SOX/GLBAといった規制上の要件を順守できるようにします。WatchGuardを代理しているパートナーは120カ国に渡り15,000社以上あります。WatchGuard本社は米国ワシントン州シアトルに所在し、北米、南米、ヨーロッパ、アジアパシフィックにもオフィスを構えています。詳細につきましてはwww.watchguard.comをご覧ください。

同資料における表現に保証はありません。全仕様書は変更される可能性があり、今後の製品や機能などの利用状況については弊社の意向に基き提供します。©2010 WatchGuard Technologies, Inc.無断複写・転載を禁じます。WatchGuard、WatchGuardロゴ、WatchGuard ReputationAuthorityはいずれも米国およびその他の国々においてWatchGuard Technologies, Inc.の登録商標あるいは商標です。その他すべての登録商標および商標は各所有者に権利があります。Part No. WGCE66719_100410