



Take Back Control: Increase Security, Empower Employees, Protect the Business

Application Control White Paper

October 2010

Introduction: Balancing Productivity with Security

As workers find new and creative ways to use the web, organizations struggle to maintain control of the corporate network while empowering employees, partners, and other stakeholders with access to critical functionality. A staggering number of new applications have emerged and the number grows daily. Complicating matters is the fact that what is considered a "good" versus "bad" application is no longer a clear-cut issue. Some applications are intended purely for business purposes and are carefully designed to minimize security risks and maximize productivity. At the other end of the risk continuum are applications programmed to steal data, corrupt computers, and disrupt network activity. A huge variety of applications fall into the gray area between these extremes.

Application Evolution Complicates Security

While IT administrators were once apt to deny access to applications whose origins were found in the consumer world, such an approach is increasingly problematic. After all, applications such as Facebook have proven quite valuable for many in the business world, particularly sales and marketing groups. In fact, 1.5 million local businesses maintain active pages on Facebook. (For this and other interesting Facebook facts, see <http://www.digitalbuzzblog.com/facebook-statistics-facts-figures-for-2010/>). At the same time, Facebook games can be productivity zappers, and if they contain malware, they also pose a security risk.

This evolution is causing administrators to reassess how they configure firewalls in protecting the corporate environment. A few years ago, IT administrators could deny access to applications by defining firewall policies blocking certain ports or protocols. But because many applications today appear as web traffic over port 80 or 443, this approach is no longer sufficient or effective. As a result, administrators have lost a fair amount of control over the applications being used across the enterprise.

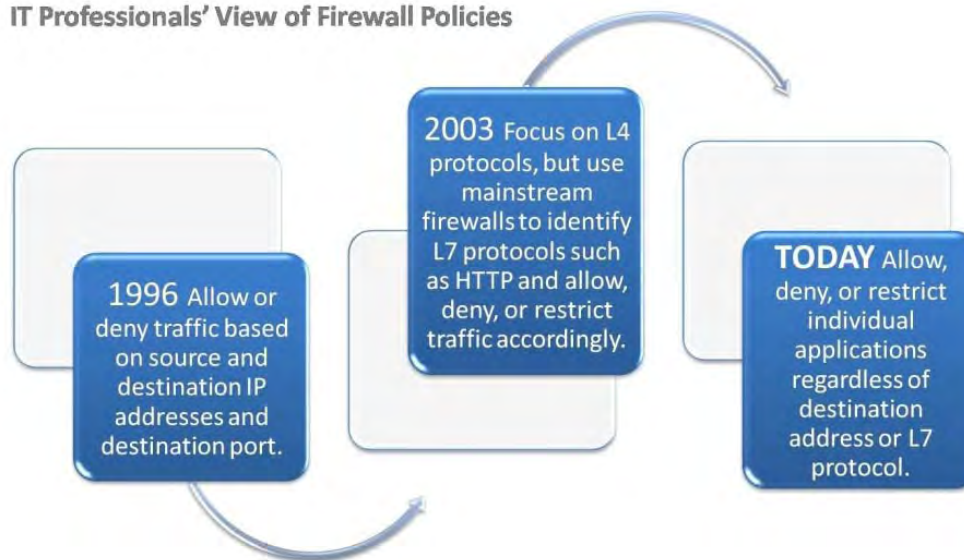
Instant Messaging (IM) and peer-to-peer (P2P) applications are prime examples of why new levels of control are required. The first generation of these applications could be regulated through basic access control lists

(ACLs) based on fixed or limited destination ports and readily identified registration servers. Second-generation applications used dynamic ports and registration servers that changed addresses frequently or were mirrored so extensively as to render ACLs less effective for blocking applications. The current generation of IM and P2P applications often act like web traffic and, in many cases, dispense with registration servers altogether. As a result, they are increasingly adept at evading firewalls. In fact, some applications – including Ultrasurf, Skype, and Winny – dodge security technologies by design. Clearly businesses need to closely control access to these applications, especially those organizations bound by certain industry regulations.

IT Administrators Need to Take Back Control

The timeline below helps illustrate what capabilities today's security professionals seek in a solution.

IT Professionals' View of Firewall Policies



To secure today's corporate environments and take back control, administrators need to identify and determine whether applications are being used for legitimate business, are malware, or fall in the gray area in between. In the latter case, IT professionals need the ability to control who can access the applications and for what purposes. Web 2.0 applications such as streaming media and audio can consume large amounts of expensive corporate bandwidth. Plus, corporations in regulated industries may need to restrict the usage of Instant Messaging because they cannot comply with requirements for electronic message retention. As part of a security and regulatory compliance posture, a corporate acceptable use policy, or a combination of the two, organizations must control employee use of the full range of applications.

The Security Risk Posed by Applications

The web is the primary source of security threats to organizations today, and web applications are often the main focus of attackers. At the same time, social networks are growing rapidly and new Web 2.0 sites are cropping up left and right. Users are often still unsure of how to exercise the appropriate levels of privacy on such sites. As a result, hackers find it convenient to use social networks as a launch pad for social engineering attacks against employees in an organization. Users are more likely to trust a link to a site when it is provided by a connection in their social network, not realizing that such accounts can easily be spoofed or faked.

Given that web traffic and web applications are the source of so many security risks, IT administrators can cut down the potential threat vectors by limiting their users to only those applications that are necessary for business purposes.

WatchGuard Application Control

WatchGuard continually evolves its solutions to keep pace with the newest challenges facing organizations of all sizes.

WatchGuard's XTM appliance v11.4 (and higher) includes Application Control capabilities that empower administrators to exercise fine-grained control over hundreds of applications, and understand which applications are being used and by whom.

The WatchGuard Application Control is a fully integrated security subscription for all WatchGuard XTM appliances. It provides global and policy-based monitoring and blocking of over 1,500 unique web and business applications for greater productivity and enhanced security. Administrators can enforce acceptable use policies for users and groups by category, application, and application sub-functions. For example, they can define a policy that allows the marketing department to access Facebook, but not Facebook games.

Using over 2,300 signatures and advanced behavioral techniques, Application Control also gives the administrator real-time and historical visibility into the use (or attempted use) of applications on the network. This level of control and visibility helps organizations enforce acceptable use policies that are mandated by industry regulation, legal and political jurisdictions, corporate goals or culture, and the like.

How WatchGuard Application Control Works

Within the WatchGuard XTM configuration tool, the administrator sets up a global policy or a more granular one covering specific users, groups, networks, or other criteria that determines which applications can and cannot be used. In real time, WatchGuard XTM with Application Control then inspects traffic crossing the appliance and determines which application is producing the traffic. Signature-based technology combined with an engine that assesses application behavior enable the appliance to identify applications with a high degree of accuracy. The appliance enforces the policy defined by the administrator and logs its actions for review. The administrator can log into the reporting GUI to see application usage, such as which applications users ran (or attempted to run) and the top applications used across the business.

The Dangers of the World Wide Web

40,000 websites are compromised per week, and 0.7% of Google Search results display sites that have been infected by malware. Source: [Google Security Blog](#), August 25, 2009.

Attacks against web applications constitute more than 60% of the total attack attempts observed on the Internet. Source: [SANS Top 10 Security Risks](#), September 2009.

64% of people interviewed by AVG click on links provided by community members in social networks, and 26% share files within social networks. Source: AVG, Social Engineering: Hacking people, not machines, 2009

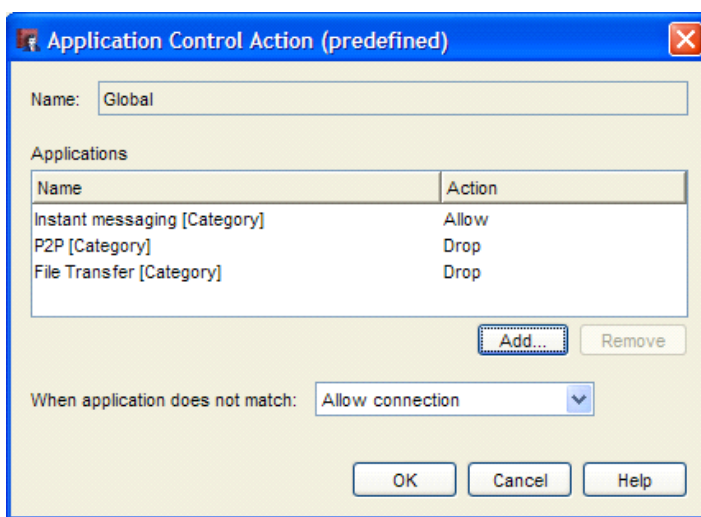


Figure 1. Administrators can easily maintain global policy settings across corporate network.

| 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-D... | Firebox | None | tcp:443 |
| 6 | ✓ | RDP | RDP | Any-External | 192.168.54.64 -> 50.50.50.50 | None | tcp:3389 |
| 7 | ✓ | WatchGuard Authentication | WGAuth | Any-Trusted Any-Optional Any-F | Firebox | None | tcp:4100 |

Figure 2. Administrator can exercise fine-grained control over hundreds of applications, organized by category, with the ability to control who uses which applications and when.

With WatchGuard Application Control, businesses can exercise granular control over the use of applications on the corporate network. For example, they can:

- Block usage of YouTube, Skype, and QQ
- Block usage of all P2P applications for users who are not part of the management team
- Allow the marketing department access to social networking sites such as Facebook and Twitter
- Allow use of Windows Live Messenger for instant messaging, but disallow file transfer over Windows Live Messenger
- Limit streaming media application usage to specific hours
- Report on the top ten applications used in the company
- Report on the use (or attempted use) of applications by any individual in the company

What to Look for in Application Control

When it comes to application control, the following are key criteria to seek in a solution:

- **Granular control.** To address the varied ways that people can use applications, it's critical to control one or more aspects of an application while being able to disallow other aspects of it. Examples of this are allowing the use of Windows Live Messenger for instant messaging but not for file transfer, or allowing access to Facebook but not to Facebook games.
- **Breadth of application signatures.** Look for an extensive list of signatures that is updated and maintained over time by the vendor. Ideally, as new applications are released and application behaviors change, signatures should be automatically updated without requiring an upgrade of the entire security application.
- **Ability to identify encrypted applications.** Today's savvy application programmers attempt to bypass security measures by encrypting application data and traffic as it traverses the Internet. The best solution uses behavior analysis to discover even well disguised applications.

Web-based Applications Reach Far and Wide

Instant Messaging

QQ, Windows Live Messenger, Yahoo! Messenger, GoogleTalk

Email

Hotmail, Gmail, Yahoo, Microsoft Exchange

Web 2.0

Facebook, LinkedIn, Twitter, Salesforce

Peer to Peer

Gnutella, Foxy, Winny, BitTorrent, eMule

Remote Access Terminals

TeamViewer, GoToMyPC, Webex

Database

Microsoft SQL, Oracle

File Transfer

Peercast, Megaupload

Voice over IP

Skype

Streaming Media

QuickTime, YouTube, Hulu

Network Management

Microsoft Update, Adobe, Norton, McAfee, Syslog

Tunnel (Web bypass proxies)

Avoidr, Ultrasurf, Circumventor

- **Incorporation into the policy set.** It's not sufficient to use add-on capabilities within an intrusion prevention service to address a few applications. Seek a solution that allows application controls to be set as part of basic firewall policies.
- **Balance of performance with efficacy.** Some products that offer application control require expensive hardware to provide acceptable levels of performance. Businesses must ensure that their security products offer high performance at a reasonable cost, along with the application control efficacy they demand.

Benefits to IT Administrators and the Business

By employing Application Control from WatchGuard, organizations will realize a variety of benefits. In addition to regaining control over the corporate environment, IT administrators actually have more power over applications than in the past. As a result, they can keep pace with the ever-evolving application universe and satisfy corporate and user demands. In fact, by applying policies that control application usage, administrators ensure employees and others can conduct their work as needed, that they stay focused and productive, and avoid potential legal problems associated with the use of unauthorized applications. Just as important, with comprehensive application control in place, organizations can be certain of limiting their security risks and preserving corporate bandwidth for applications and usage consistent with corporate objectives.

WatchGuard XTM: A Full-Featured Firewall for Application Control

As employees, partners, and others within the corporate environment have ready access to a variety of applications, organizations must find ways to balance user needs with security. Now that so many applications defy clear-cut categorization, IT administrators require new levels of control over which applications are allowed and by whom.

This type of application control is available in the WatchGuard XTM firewall today. WatchGuard delivers it as part of a full-featured firewall that includes all the functionality needed to easily, comprehensively, and cost-effectively secure the corporate environment. In addition to advanced application-based policy construction and enforcement, XTM supports all of the traditional port- and protocol-based configurations that administrators are familiar with, along with critical networking features, including dynamic routing, WAN failover, and load balancing. A drag-and-drop VPN method makes it easy to create site-to-site tunnels for secure connections between locations. Moreover, a suite of interactive, real-time monitoring tools save time and make it easy to see at-a-glance information about user, network, and security activities.

Moreover, on top of providing industry-leading price/performance, WatchGuard XTM offers a number of other security subscriptions that deliver comprehensive threat management capabilities:

- **Reputation Enabled Defense:** Delivers a powerful cloud-based URL reputation service that protects web users from malicious web pages, while dramatically improving web throughput.
- **spamBlocker:** Blocks unwanted email with near 100% accuracy along with the viral payloads that spam often carries. spamBlocker recognizes spam regardless of the language, format, or content of the message – even image-based spam that other anti-spam products often miss.
- **WebBlocker:** A URL filtering service that blocks access to dangerous and inappropriate web sites in the workplace. It filters URLs on both HTTP and HTTPS to close the HTTPS loophole many other web filters leave wide open.
- **Gateway AntiVirus:** Provides powerful signature-based protection at the gateway against known viruses, trojans, worms, spyware, and roguesware.

- **Intrusion Prevention:** Scans all ports and protocols to block attacks that comply with standard protocols but carry malicious content, including buffer overflows, SQL injections, and remote file inclusions.

Find out more about WatchGuard Application Control and the XTM family of network security appliances, visit, www.watchguard.com, contact your local reseller, or call WatchGuard directly at 1.800.734.9905 (U.S. Sales) or +1.206.613.0895 (International Sales).

ADDRESS:

505 Fifth Avenue South
Suite 500
Seattle, WA 98104

WEB:

www.watchguard.com

U.S. SALES:

1.800.734.9905

INTERNATIONAL SALES:

+1.206.613.0895

ABOUT WATCHGUARD

Since 1996, WatchGuard Technologies has provided reliable, easy to manage security appliances to hundreds of thousands of businesses worldwide. WatchGuard's award-winning extensible threat management (XTM) network security solutions combine firewall, VPN, and security services. The extensible content security (XCS) appliances offer content security across email and web, as well as data loss prevention. Both product lines help you meet regulatory compliance requirements including PCI DSS, HIPAA, SOX and GLBA. More than 15,000 partners represent WatchGuard in 120 countries. WatchGuard is headquartered in Seattle, Washington, with offices in North America, Latin America, Europe, and Asia Pacific. For more information, please visit www.watchguard.com.

No express or implied warranties are provided for herein. All specifications are subject to change and any expected future products, features, or functionality will be provided on an if and when available basis. ©2010 WatchGuard Technologies, Inc. All rights reserved. WatchGuard and the WatchGuard logo are either trademarks or registered trademarks of WatchGuard Technologies, Inc. in the United States and/or other countries. All other trademarks and tradenames are the property of their respective owners. Part No. WGCE66719_100410