Adding Application Control to Your Security Toolbox

Solution Guide

Application control to stop threats, mitigate loss of productivity and bandwidth, and reduce liability and compliance risks.

FORTINET®

Executive Summary

The corporate application landscape is steadily expanding. Many factors have combined to fuel this growth: the ubiquity of the Internet and associated protocols, the ongoing transition of enterprise applications to web platforms, and the steady increase in easily installed web 2.0 and personal applications (e.g., web mail, IM, Facebook, and file sharing). One result of this expansion is the increasing potential application-borne threats have to evade security countermeasures. Another is to require that IT staff stay vigilant to productivity, bandwidth, and liability and compliance issues.

Application control is one such tool. It enables administrators to accurately identify and control applications based on their behavior, even when disguised or tunneling through other protocols. When delivered as part of a multi-layered approach to network security, application control not only improves your ability to ward off malicious activity, but also mitigates the impact of user-installed software on both bandwidth and productivity (user, help desk, and IT staff), and assists in controlling liability and compliance risks.

This solution guide offers suggestions on how to get the most out of implementing application control in your network. After discussing the expanding applications frontier and its impact on an enterprise, the paper defines application control and reviews the requirements it must meet to deliver the capabilities noted above. There follows an overview of application control in Fortinet FortiOS 4.0 as the basis for the concluding section, which discusses Fortinet technology that allows you to implement application control.

The Expanding Applications Frontier

Network security is demanding more and more effort as IP connectivity continues to transform communications. Business networks depend on an ever-increasing array of protocols, including HTTP, P2P, to coordinate intra- and inter-application activity. Users can access or download a bewildering variety of personal applications, such as web email, IM, free VoIP, P2P, browser toolbars, and various social media. They have become accustomed to accessing these sites or installing applications on their personal computers, and often install them on their business computers as well. The popularity of many of these applications has led many organizations to use social media applications as part of their overall marketing and communications plans. In addition, initiatives to increase accessibility to applications and data make it increasingly difficult to specify the locations where users will need access to corporate information, or who will need access: users, partners, customers, franchisees, or agents—the list keeps growing.

Traditionally, most enterprises have relied on their firewalls to enforce application policies. They established the primary line of defense at the network perimeter by regulating what type of traffic the firewall permits, blocking ports and thereby blocking unwanted applications. For example, if an enterprise had a policy in place against establishing FTP connections with clients outside the firewall, it could enforce that policy by blocking outbound traffic on ports 20 and 21.

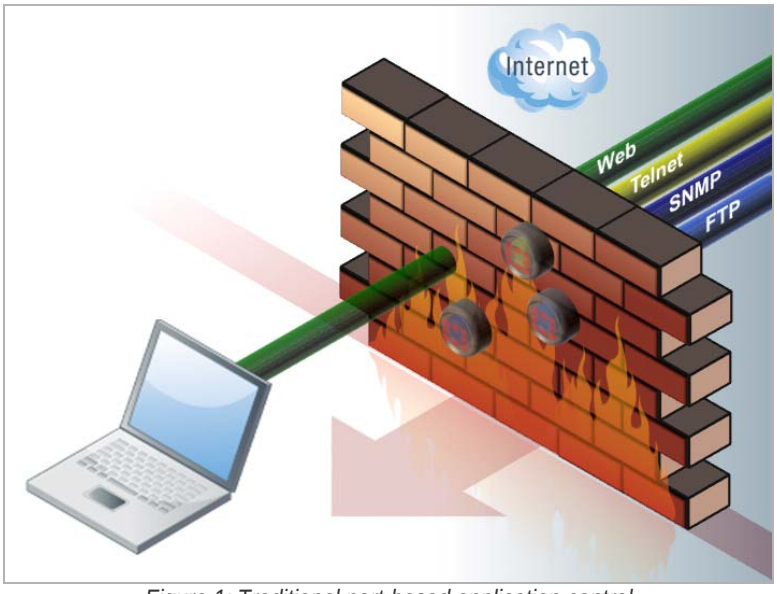

Figure 1: Traditional port-based application control

However, the result of this expansion of applications in enterprise environments is a dramatic increase in the potential for application-borne threats to evade security traditional countermeasures like firewalls. There are several reasons for this increase in exposure:

- Protocols: Many applications running in enterprise environments are extremely sophisticated and able to deliver dynamic content and services. They communicate with other systems using a variety of HTTP, proprietary, and common protocols, preventing static rule sets from enforcing application usage policies.
- Development: With the rapid evolution and adoption of web 2.0-style features in business applications, the use of browsers (HTTP) in enterprise applications is now an acceptable development practice. Only a few years ago, application development required a custom application (which usually required proprietary protocols), facilitating policy enforcement.
- Deployment: Enterprises have a range of application deployment options available. They can utilize on-premise, hosted, or virtual deployment (or any combination thereof) making it difficult to differentiate legitimate content from malicious content.

HTTP is the protocol that causes the greatest challenge to policy enforcement and application control. It is now both the highway for critical business applications, as well a common threat delivery mechanism. The ever-expanding network of connected locations (including mobile devices) and users (including partners, customers, franchisees, and agents) rely on HTTP-based applications. This reliance on HTTP traffic enables application-level threats to evade firewall-based policies because the firewalls do not discriminate between legitimate and illegitimate web traffic. As Figure 2 illustrates, Enterprises cannot simply block port 80 because of the volume of data that arrives via HTTP.

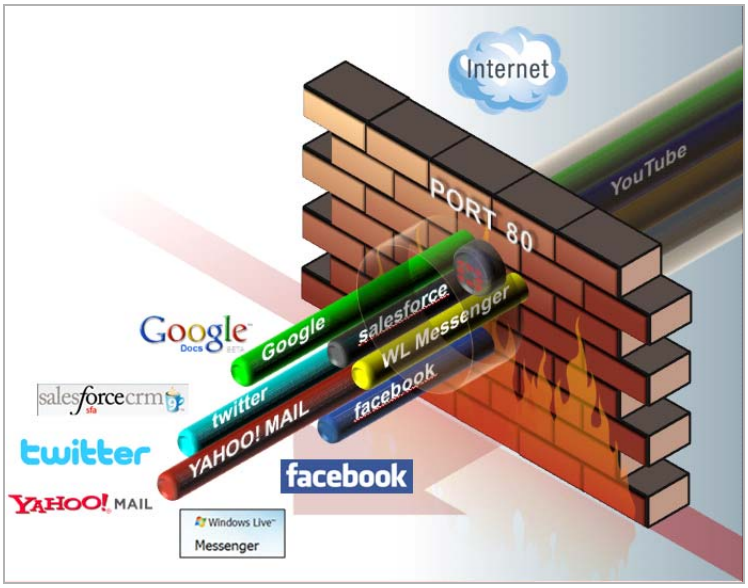

Figure 2: Applications using HTTP bypass firewall-based application control

The effect of being unable to control HTTP-based applications goes beyond threat delivery. Not only can they punch holes in network security, but they can also increase both operating and capital expenditures by:

- Distracting users from productive activity (AOL Instant Messenger, Google.Talk, MSN, QQ, Yahoo Messenger),
- Consuming network bandwidth (BitTorrent, eDonkey, YouTube)
- Exposing your organization to security, liability and regulatory compliance risks (Remote Desktop, PCAnywhere, VNC)

Table 1 illustrates the new applications frontier by grouping it into 18 categories, and indicating the primary impacts they are likely to have on an enterprise.

Table 1: Applications and Protocols

Application Categories	Sample Applications	Impact		
		Loss of Productivity	Network Bandwidth Consumption	Security/Liability/ Compliance Risk
Instant Messaging	AIM, Google.Talk, MSN, QQ, Yahoo	Yes	Yes (Voice/Video)	Yes
Peer-to-peer	BitTorrent, Edonkey, Gnutella, Kazaa, Skype	Yes	Yes	Yes
Voice over Internet Protocol	H.245, MGCP, Net2phone, Netmeeting, SIP.TCP	Yes	Yes	Yes
File Transfer	FTP, HTTP.Audio, HTTP.EXE, RapidShare, YouSendIt		Yes	Yes
Video/Audio Streaming	Itunes, Peercast, PPStream, Quicktime, RealPlayer	Yes	Yes	Yes
Internet Proxy	Ghostsurf, Hamachi, HTTP.Tunnel, Tor.Web.Proxy, Ultrasurf	Yes	Yes	Yes
Remote Access Connection	Gotomypc, MS.RDP.Request, PCAnywhere, Teamviewer, VNC.Request			Yes
Games	AIM.Game, KnightOnline, MSN.Game, PartyPoker, Second.Life, WorldofWarcraft	Yes	Yes	Yes
Web Browser Toolbar	Alexa.Toolbar, AOL.Toolbar, Mcafee.SiteAdvisor, MSN.Toolbar, Yahoo.Toolbar	Yes		Yes
Database	DB2, MSSQL, MySQL, Oracle, Postgres, Sybase			Yes
Web-based email	AIM.Webmail, Gmail, Hotmail, MySpace.Webmail, Yahoo.Webmail	Yes		Yes
Web	Amazon, Ebay, Facebook, Google.Safe.Search.Off, Myspace, Wikipedia	Yes	Yes	Yes
Protocol Command	FTP.Command, HTTP.Method, IMAP.Command, POP3.Command, SMTP.Command			Yes
Internet Protocol	ICMP, IGMP, IPv6, L2TP, RDP, RSVP			Yes
Network Services	LDAP, MSRPC, RADIUS, SSH, SSL, Telnet			Yes
Enterprise Applications	Centric.CRM, IBM.Lotus.Notes, Salesforce, SugarCRM, Webex.Weboffice			Yes
System Update	Adobe.Update, Apple.MacOS.Update, McAfee.Update, Microsoft.Update, TrendMicro.Update	-	Yes	
Network Backup	Big.Brother, CA.MQ.Backup, Ibackup, IBM.Tivoli.Storage.Manager, Rsync		Yes	Yes

Note: Additional information, including a searchable database of applications, is available without cost at www.fortiguard.com.

Reining In Users

Those organizations aware of the impacts cited above implement computer use policies of varying strictness to reduce their exposure to risk. Unfortunately, there are technical and political difficulties in enforcing those policies. On the technical side, most firewalls and intrusion prevention systems (IPS) have not been able to distinguish reliably between the applications that are using HTTP tunneling. Many of these personal-use applications have evolved to evade security countermeasures. The applications employ techniques such as random port-hopping (such as BitTorrent) and tunneling via other protocols besides HTTP (such as SSL and P2P). Web filtering can stop access to a web page, but it cannot control applications launched by that page. In addition, users may try to evade web filtering technologies by using Internet proxies, such as GhostSurf and Hamachi. These proxies make it impossible to discern the Internet site they which are connecting. In highly regulated or high-liability industries in particular, evasion techniques like these can mandate costly security measures. These countermeasures can consume IT budget needed for new initiatives, as well as negatively affect user productivity.

On the political side, many organizations calculate that it is neither cost-effective (due to the technical constraints cited above) nor good for employee morale to clamp down entirely on user applications. In fact, a recent study by the University of Melbourne found that users who indulged in what the researchers called Workplace Internet Leisure Browsing (WILB) are more productive than those who do not. The study noted that those who limit such WILB activity to less than 20% of their total time in the office are more productive by about 9% than those who do not.[1]

In such cases, IT must often plan and budget for both discretionary bandwidth for personal applications and non-discretionary bandwidth for business applications. Unfortunately, without the ability to discern between them, control is very difficult, and such plans are often no more than empty wishes.

Beyond Security: Application Control

Application control overcomes these problems by accurately identifying and controlling applications even when disguised by port-switching or tunneling through other protocols. Application control makes this identification based on the packets' behavior as revealed by deep packet inspection and advanced protocol decoding. A traditional firewall controls traffic by the service (or port); application control builds on firewall technology by adding a more dynamic inspection of each traffic stream to identify the application and not only pass or block it, but also apply a variety of other actions or policies, such as traffic-shaping. Thus, application control adds the ability to manage and audit authorized traffic to the ability of firewalls and IPS to detect and block unauthorized traffic. By increasing the granularity of a security solution, application control broadens the IT staff's ability to manage protocols and applications to deliver the most business benefit at the least risk. It also enables enterprises to permit specific personal-use applications for business productivity.

It is important not to think of application control in isolation from all the other countermeasures available to security organizations. These include firewalls, virtual private networks (VPN), IPS, antivirus/antimalware (AV/AM), and web filtering. To do so is to fall into a reactive mindset, in which the IT staff deploys point solutions as new types of threats emerge. Enterprises in particular have suffered from this approach by deploying stand-alone technologies. Reactive security is more costly in terms of hardware, and much more difficult to manage. It increases operating costs, and makes it difficult, if not impossible, to respond effectively to increasingly dangerous blended threats.

Another drawback to adding multiple layers of security is the effect on network performance. Deploying a series of independent countermeasures would sacrifice network performance, as each stand-alone process requires separate inspection of each packet. This redundant packet inspection would inject significant amounts of latency into data throughput.

Instead, to realize its full potential, enterprises must implement application control as part of a multi-layered solution that combines all these security tools into a system. This integrated approach not only yields in-depth protection, but also makes it easier to deploy and manage, thereby reducing the burden on IT staff and frees up IT resources for new initiatives. The development of such comprehensive threat management systems is certainly the industry trend. According to Gartner, by 2010, only 10% of emerging security threats will require tactical point solutions, compared with 80% in 2005.[2]

As part of a multi-layered system, application control offers organizations more control because it overlaps with other important security technologies. These other technologies can either function as an additional check on applications authorized by the application control, or use application control for more control over the network traffic they authorize.

Consider just two examples of how application control fits into an integrated security strategy. For instance, Figure 3 illustrates how integrating AV with application control offers the benefit of additional protection by detecting malicious activity in applications authorized by application control policies.

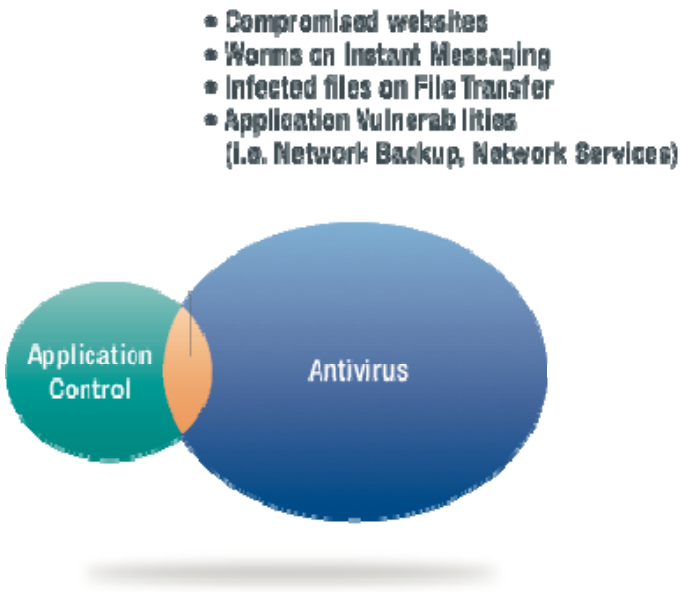

Figure 3: Additional protection offered by combining application control with antivirus

Figure 4 shows how the ability of application control to "see" applications tunneling through HTTP yields additional protection with sites or pages that web filtering authorizes.

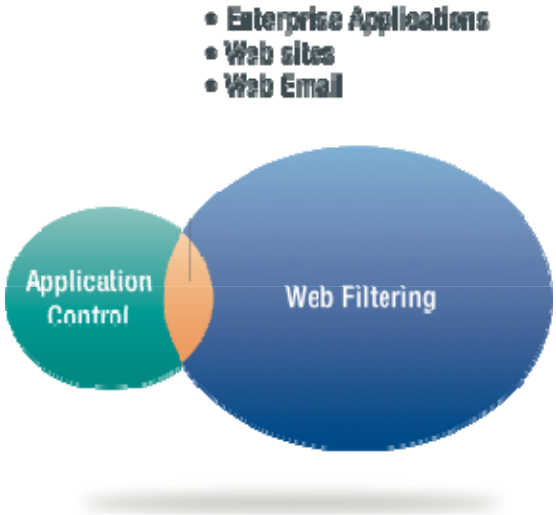

Figure 4: Additional protection offered by combining application control with web filtering

The Fortinet Approach—Integrated Security without Compromise

Fortinet offers an alternative to the unpleasant choice facing enterprises: Adding increased layers of protection or maintaining performance of data and applications. Fortinet's custom-built FortiGate® platforms deliver integrated, high-performance security technologies that provide defense-in-depth against malicious or unwanted applications without sacrificing network performance. FortiGate platforms exceed the performance and functionality of other security systems running on modified versions of standard operating systems and off-the-shelf processors.

FortiGate appliances are based on an integrated hardware and software architecture specifically designed for high-performance application-level content processing in perimeter, core, and data center networks to provide real-time security functions at multi-gigabit per second data rates. There are two key components to FortiGate appliances:

- FortiOS™ is the security-hardened operating system directs the operations of processors. It provides system management functions and unified interface for managing the range of security functions in the FortiGate platform. Enterprises can selectively enable FortiOS security services to provide a unique set of services or a full suite of UTM security services all within a single platform. Fortinet's FortiGuard™ network dynamically updates the FortiOS and the protection services it provides, ensuring maximum protection for antivirus, antispam, web filtering, antispyware, and intrusion prevention.
- FortiASIC™ is the foundation of Fortinet's unique hardware technology. It is a family of purpose built, high-performance network and content processors that work with a general-purpose processor to accelerate process-intensive security services. FortiASIC provides the performance required to deliver enterprise-class threat management services. FortiASIC, using Fortinet's patent pending Content Pattern Recognition Language (CPRL), delivers the highest levels of performance whether providing a single service or an entire suite of UTM security services. The FortiASIC-CP is a key component in all FortiGate security platforms. It provides a hardware scanning engine, hardware encryption, and real-time content analysis processing capabilities. The FortiASIC-NP series of processors provides acceleration for firewall, encryption/decryption, signature and heuristic packet scanning, and bandwidth shaping.

FortiOS 4.0 Application Control: Security-Plus

Fortinet FortiOS 4.0 is the foundation for the operation of all FortiGate appliances, from the core kernel functions to security processing features, including application control. Like virtually all of the other security tools in Fortinet solutions, application control leverages several long-time FortiOS capabilities, including the IPS scan engine and signatures, proxy support, and rate limiting. Application control adds a dynamic application identification engine that recognizes applications based on their behavior. With this addition, you gain the ability to defend against application vulnerabilities and attacks that are largely platform-independent, as well as the platform-dependent threats IPS guards against.

In FortiOS 4.0, the integration of application control adds key functionality to the FortiGate platforms:

- Port-independent detection: Application control can detect an application regardless of the TCP/IP ports on which it may be running, such as HTTP and SSL over non-standard ports (80 & 443), or SSH connection using pre-determined port, or SSL MS SQL Database that is not on port 1433.
- Tunneling detection: Leveraging the proprietary pattern matching of FortiOS 4.0, application control can identify applications tunneling via other applications. For instance, it can detect applications such as Skype and BitTorrent that use HTTP tunneling to evade firewalls.
- The FortiGate application identification database: It currently contains more than 1,000 signatures for applications and protocols in the 18 categories referenced in Table 1 above, based on the work of application experts in the FortiGuard® Global Threat Research Team. FortiGuard Security Subscription Services automatically supplies updates to the database.
- Fine-grained control: Application control provides highly granular control over applications, down to the level of individual user IDs. This gives administrators the ability to enforce application access and use policies based on user roles or by department or business unit.
- Customizable actions plus traffic shaping: Actions include block, pass, and traffic shaping for bandwidth control. You can block operations within applications, such as PUT for FTP. For IM, application control can block file transfers, or, by leveraging FortiOS antivirus/antispyware/antimalware capabilities, inspect for malicious files if policies allow for file transfer. It can also archive the content of IM messages to assist with regulatory compliance. Rate limiting is available for some P2P applications.
- Easy management: Integration of application control extends to the FortiOS management interface, which makes it possible to define application control policies in combination with firewall and IPS policies, yielding more thorough coverage with less effort than point solutions or less-integrated offerings.
- Flexible reporting: Available via FortiAnalyzer, this capability categorizes traffic by ports, protocol, or applications and enables you to audit your network to discover what applications are actually running on it. You can identify top applications, top applications in each category (as described in Table 1 above), top users for each top application, and much more. This is not only the critical first step of effectively planning and implementing application control on your network, but also a never-ending task in your ongoing effort to manage the constantly changing mix of protocols, applications, and threats that are the reality of IP networking today.

Conclusion

The wide range of applications found in today's enterprise environments present significant challenges for enforcing security policies. The proliferation of HTTP-based communications, both business-critical and for personal use, limits the effectiveness of a firewall's port-based policy enforcement. Application-layer threats can evade firewall-based policies due to the firewall's inability to differentiate between legitimate and malicious traffic. Unwanted or malicious applications also can expose enterprises to decreased productivity, decreased network bandwidth, and increased liability and regulatory compliance risks.

Enterprises need additional layers of protection, such as IPS, antivirus/antimalware, web filtering and application control, to provide complementary, overlapping layers of protection against malicious and unwanted applications. To maximize the effectiveness of these additional security technologies, you need to deploy them in a single, integrated platform. A single platform minimizes operational and capital expenses while maximizing effectiveness.

Fortinet's custom-built FortiGate platforms deliver integrated, high-performance security technologies that provide defense-in-depth against malicious or unwanted applications without sacrificing network performance. FortiGate platforms are purpose-built, combining the power of the proprietary FortiOS security operating system with the proprietary FortiASIC network and content processors. FortiGate platforms deliver proven, integrated protection without compromise.

About Fortinet

Fortinet protects customers against application and network threats. It is the pioneer and leading provider of unified threat management security systems. Enterprises of every size, including service providers and carriers, rely on Fortinet platforms to increase their security while reducing total operating costs. Fortinet built its ASIC-accelerated solutions from the ground up to integrate multiple levels of security protection, including firewall, antivirus, intrusion prevention, VPN, spyware prevention, anti-spam, application control, WAN optimization, web filtering, SSL inspection, and data loss prevention. Leveraging a custom ASIC and operating system, as well as unified interface, Fortinet solutions offer advanced security functionality that scales from remote office to globally distributed environments with integrated management and reporting. Fortinet solutions have won multiple awards around the world and are the only security products that are certified in six programs by ICSA Labs: (Firewall, Antivirus, IPSec, Network IPS, and Anti-Spyware). Fortinet is privately held and based in Sunnyvale, California.

FORTINET
1090 Kifer Road, Sunnyvale, CA 94086 USA
Tel +1-408-235-7700
Fax +1-408-235-7737
www.fortinet.com

WPR142-R1 0909

[1] University of Melbourne: Freedom to surf: workers more productive if allowed to use the internet for leisure (http://uninews.unimelb.edu.au/news/5750/)
[2] Gartner: Cost Cutting While Improving IT Security, March 20, 2008