FORTINET®

SOLUTION GUIDE

Controlling Web 2.0 Applications in the Enterprise

Summary

New technologies used in Web 2.0 applications have increased the volume and complexity of network traffic internal to organizations and at Internet gateways. More than ever, it's important for businesses to deploy new methods of monitoring and controlling these Internet-based applications in order to discover and mitigate hidden security threats.

Introduction

Applications are the lifeblood of today's organizations as they allow workers to perform crucial business tasks. When granted access to enterprise networks and the Internet, applications can enable sharing of information within workgroups, throughout an enterprise and externally with partners and customers. Not long ago, when applications were launched only from desktop computers and servers inside the corporate network, data security policies were relatively easy to enforce. However, today's organizations are grappling with a new generation of security threats. Consumer-driven technology has unleashed a new wave of Internet-based applications that can easily penetrate and circumvent traditional network security barriers.

Better known as "Web 2.0" applications, these new Internet-based communications tools such as Facebook, Twitter and Skype have already achieved widespread penetration inside organizations. Inevitably, these new Internet-based technologies and applications have spawned a new set of challenges for enterprises seeking to secure their networks against malicious threats and data loss. Allowing employees to access Web 2.0 applications has made enforcing data security policies a far more complex problem. Even worse, many businesses have no way to detect, much less control these new applications, increasing the potential for intentional or accidental misappropriation of confidential information.

Application Control Challenges

Web 2.0 applications enable instantaneous, always-on communications between employees, partners and contractors, bringing great leaps in productivity. As a result, many organizations have integrated instant messaging, Twitter feeds and Facebook pages into their everyday business practices. However, these new applications bring security concerns because they can tunnel through trusted ports, use proprietary encryption algorithms and even masquerade as other applications to evade detection and blocking by traditional firewalls. This makes it much easier to transfer digital information undetected and unimpeded from inside an enterprise network, and for a new generation of viruses and threats to breach traditional network firewalls.

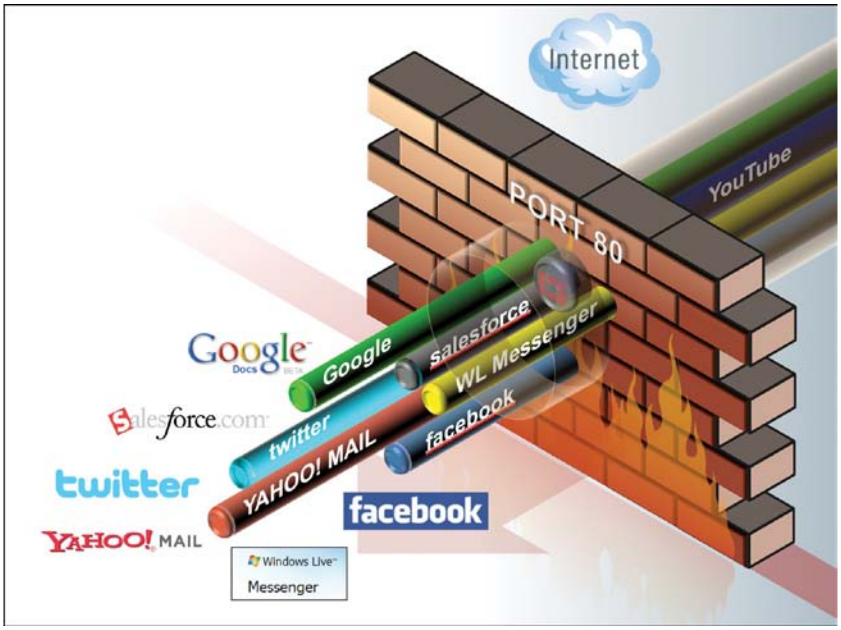


Figure 1: Web 2.0 applications passing through a traditional firewall

Loss of visibility and control

Controlling access to traditional Internet-based applications such as telnet and FTP is easily accomplished by blocking or enabling individual TCP and UDP ports at the network gateway. Today, multiple applications can use the same port, while single Web 2.0 applications sometimes use multiple ports. Evasive applications can use non-standard ports and SSL encryption to avoid detection and control. Even the very definition of "application" has changed. Some applications are run from inside Web browsers as plug-ins, while others run within host applications. Social media sites such as Facebook allow users to chat, watch videos, play games, and even launch other applications - all from inside the browser.

Web 2.0 applications enable new threats

Stateful firewalls that use only port and protocol blocking can fail to protect businesses against web-based threats such as the Koobface virus. Koobface is a computer worm that targets users of social networking applications including Facebook, Twitter and Friendster. When an unsuspecting user clicks on a link to download a video or other media, they are in fact installing the Koobface "bot" or botnet client. Bots can initiate malicious services from infected computers by forming global botnets through communication with other bots, or by "phoning home" to "command and control" (C&C) servers over the Internet. The Koobface bot uploads personal information and passwords to Koobface C&C servers[1], and also directs users to other malicious sites where additional malware can be downloaded. Among the components downloaded by the Koobface virus are DNS filter programs that can block access to well known security sites, and a proxy tool that enables attackers to further abuse the infected computer. Other recent threats include the Sasfis, Hiloti, Bredolab and Mariposa/Butterfly bots[2].

Unintentional data breaches

Even without the assistance of web-based malware, confidential data is frequently sent to the wrong party or accidentally shared with the general public, resulting in an unintentional data breach. These accidental data breaches can expose businesses to fines from regulators, lawsuits from customers and shareholders, and negative press which can require damage control. A popular example of how data can be shared accidentally is through use of Twitter's "direct message" feature, which allows a Twitter user to send a private text message to another Twitter user. Should the recipient wish to reply confidentially, they must remember to type "dm" in front of their message, or the response will be regarded as a public "Tweet". Public Tweets are automatically sent to all of the responders' followers, and can also be viewed publicly by anyone with a Twitter account.

Need to limit bandwidth usage

Web 2.0 applications accessed from inside the enterprise - for example to stream videos or to participate in web-based games - can consume a great deal of network resources if left unchecked. Heavy use can slow mission-critical communications and applications running on a network, reducing worker productivity and forcing businesses to purchase unneeded bandwidth. In addition, events such as Michael Jackson's funeral and the World Cup soccer finals, which were closely followed and commented on using Web 2.0 applications, have overwhelmed enterprise and service provider networks worldwide. Yet many companies are reluctant to block access to these new technologies and applications for fear of limiting vital communications or alienating employees.

Traditional Application Control

Security administrators used to be able to prevent applications from transferring data outside of an organization by simply installing a stateful firewall at the network perimeter. Stateful firewalls operate at the network layer of the seven-layer OSI model, examining packet headers and keeping track of established network connections in a state table. Once a connection is established, all subsequent traffic associated with that connection is deemed safe and passed through the firewall with very limited or no further inspection.

Port blocking and URL filtering

Stateful firewalls used to be successful at blocking most applications because most applications used to communicate over networks by using specific and unchanging computer ports and protocols. When an administrator decided that an application was unsafe, they could quickly block access to it by modifying the firewall policy to block ports and protocols associated with that application. However, traditional port-based protection is no longer practical because blocking port-80, for example, would block access to the web entirely. This is simply not an option for most enterprises today.

URL filtering could also be applied at the gateway to block employee access to non-trusted web sites, as well as to traditional web-based applications such as Yahoo email. However, since many new applications communicate over the Internet through web browsers, web-based exploits and drive-by attacks are able to slip through gaps in traditional URL filtering and virus protection. In addition, web filtering is good at blocking access to entire web sites, but cannot be used to

[1] Koobface Worm Doubles C&C Servers in 48 Hours
http://threatpost.com/en_us/blogs/koobface-worm-doubles-cc-servers-48-hours-031110

[2] Security Minute: November Edition Looks at Spam Reduction, Koobface Takedown and Hiloti Trojan
http://blog.fortinet.com/security-minute-november-edition-looks-at-spam-reduction-koobface-takedown-and-hiloti-trojan/

partially block access to web-based applications. For example, some applications have valuable features that a company might wish to allow, while blocking access to other features.

New application control methods needed

A single Koobface infection could result in loss of trade secrets or identity theft, yet many organizations do not have an effective way to inspect streaming content for this type of malicious code. Clearly, organizations attempting to maintain necessary business functions while safeguarding important information will need to gain firm control of the Web 2.0 technologies and applications traversing their networks. Application control is no longer as simple as "block" or "allow". With the advent of social networks, multiple layers of protection are now a necessity.

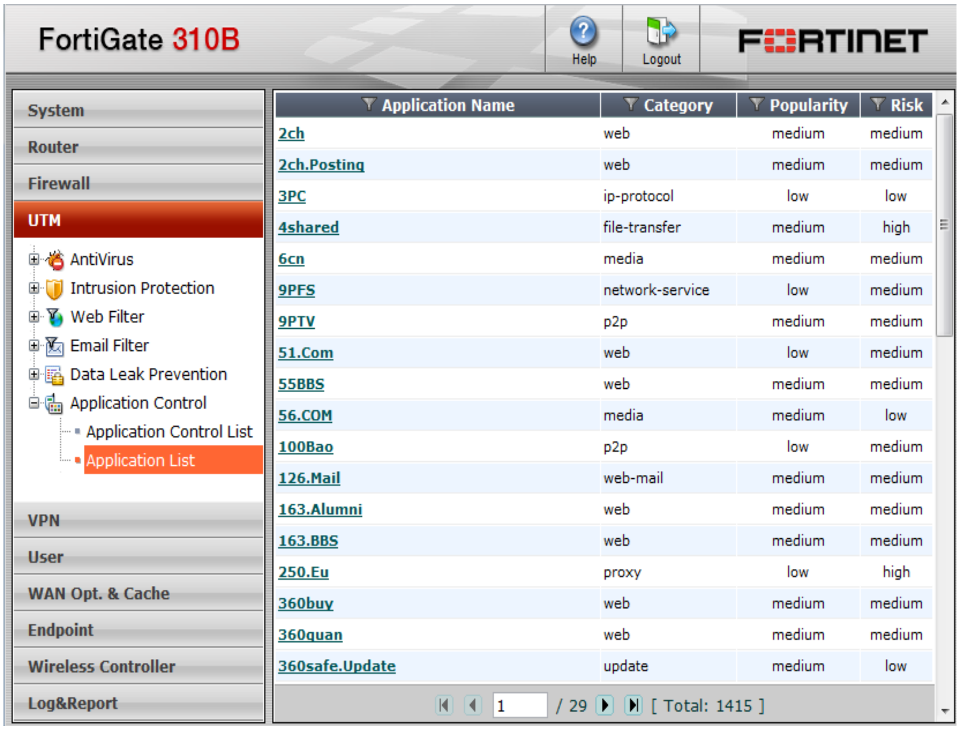
Complete Content Protection

In order to prevent data loss and mitigate new threats, organizations must be able to effectively control legacy applications as well as the new breed of Internet-based applications. They must be able to detect, monitor and control application usage and traffic at gateways and at endpoints. In addition, an association must be made between the application and the end user so that proper access rights can be assigned to the user through a security policy.

Fortinet Application Control, a security feature provided by FortiOS™, can detect and restrict the use of applications on networks and endpoints based on application classification, behavioral analysis and end user association. Applications can be denied by default or allowed on a case-by-case basis. FortiOS is the security-hardened operating system used by all FortiGate® consolidated security appliances. Some of the important features and benefits provided by Fortinet Application Control are described in the following sections.

Detecting Internet-based applications

Network traffic and applications are generally controlled at the firewall by tracking the ports used, source and destination addresses, and traffic volume. However, as explained earlier, these methods may not be sufficient to precisely define or control traffic from web-based applications. To address this problem, Fortinet Application Control uses protocol decoders to decrypt and examine network traffic for signatures unique to an application. Even when applications attempt to hide by using non-standard ports and protocols, they can still be discovered. In addition, protocol decoders enable decryption and examination of encrypted network traffic. This allows application control to be applied to IPSec and SSL-encrypted VPN traffic. Protocols that can be inspected include HTTPS, POP3S, SMTPS and IMAPS. Fortinet Application Control does not require any knowledge of server addresses or ports.



Application Name	Category	Popularity	Risk
2ch	web	medium	medium
2ch.Posting	web	medium	medium
3PC	ip-protocol	low	low
4shared	file-transfer	medium	high
6cn	media	medium	medium
9PFS	network-service	low	medium
9PTV	p2p	medium	medium
51.Com	web	low	medium
55BBS	web	medium	medium
56.COM	media	medium	low
100Bao	p2p	low	medium
126.Mail	web-mail	medium	medium
163.Alumni	web	medium	medium
163.BBS	web	medium	medium
250.Eu	proxy	low	high
360buy	web	medium	medium
360quan	web	medium	medium
360safe.Update	update	medium	low

1 / 29 [Total: 1415]

Figure 2: Fortinet Application Control

FortiGuard Application Control Database

Once network traffic is decoded, applications can be identified by their unique signatures. Fortinet Application Control leverages one of the largest application signature databases available – the FortiGuard® Application Control Database. This enables Fortinet Application Control to explicitly detect more than 1,400 unique web-based applications, software programs, network services and network traffic protocols. The FortiGuard Application Control Database is continually refreshed with signatures for new applications, as well as new versions of existing applications. FortiGuard Services deliver regularly scheduled updates to FortiGate consolidated security appliances, ensuring that Fortinet Application Control always has the latest signatures available for reference.

Application control lists

Administrators can control applications explicitly by entering them into an application control list in the firewall policy. In addition, they can create multiple application control lists, each configured to allow, block, monitor or shape network traffic associated with a unique list of applications. An application "whitelist" is appropriate for use in a high security network, as it allows only traffic from listed applications to pass through the gateway. An application "blacklist" on the other hand, blocks only listed applications. Applications can be controlled individually, or separated into categories and controlled as groups. A number of default application control lists are provided with Fortinet Application Control. These default lists can be used out-of-the-box, or customized to meet specific security requirements.

Table 1: Some default application control lists provided by Fortinet

Default List Name	Description
block-p2p	Blocks known peer-to-peer applications while allowing all other application traffic.
monitor-all	Enables application control monitoring for all traffic. Allows all application traffic.
monitor-p2p-and-media	Enables application control monitoring for applications in the peer-to-peer and media categories. Allows all application traffic.

When an application is identified through comparison with the FortiGuard Application Control Database, the policy defined in the application control list is applied. Traffic from blocked applications is dropped, conserving network bandwidth and avoiding further inspection of that traffic. Additional unified threat management (UTM) security capabilities provided by FortiOS - such as intrusion prevention, antivirus/antispyware scanning and data leak prevention - can then be applied to the remaining network traffic.

Associating the end user with applications

FortiOS provides the Fortinet Server Authentication Extension (FSAE) to associate end users with user group policies, enabling single sign-on and application control capabilities. FSAE monitors user logins and forwards the user name, IP address and list of Active Directory user group memberships to a FortiGate consolidated security appliance. When the user tries to access network resources, the FortiGate applies the appropriate firewall policy for the requested destination or application, allowing the connection only if the user belongs to one of the permitted user groups. FSAE can also identify users on networks using Windows NTLM authentication and Novell eDirectory.

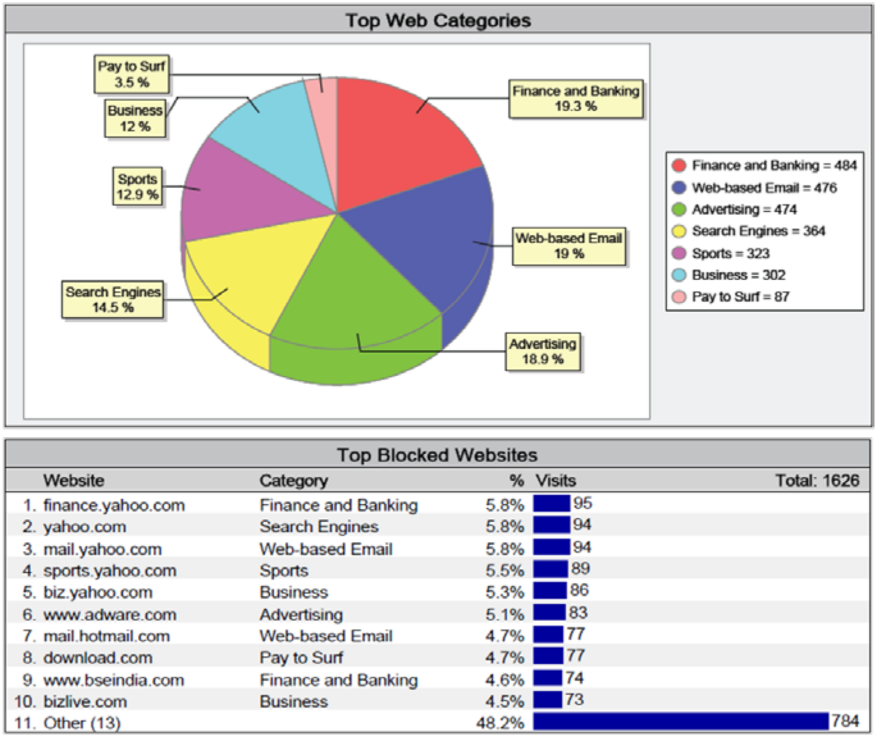
Application control granularity

Whitelists and blacklists can be used in the same policy for more granular control. Fortinet Application Control can also distinguish between multiple applications available from a single social networking site. For example, it can identify and apply policies individually to application traffic from Facebook Chat and Facebook Video. Similarly, Fortinet Application Control can apply separate policies to eighteen Google-related applications including Google search, Google Maps and Google Video. In addition, traffic shaping can be enabled to restrict network bandwidth available to some applications while giving priority to others.

Figure 3: Some popular Web 2.0 applications

Application traffic shaping

Application traffic shaping allows administrators to limit or guarantee the network bandwidth available to all applications or individual applications specified in an application list entry. For example, a business could limit the bandwidth used by Skype and Facebook chat to no more than 100 kilobytes per second, or restrict YouTube traffic to reserve network bandwidth for mission critical applications. Traffic shaping can also be configured on a time-sensitive basis to restrict user access or bandwidth available to applications during certain times of the day. Traffic shaping policies are created independently of firewall policies and application control lists so that administrators can reuse them in multiple policies and list entries. Shared traffic shaping policies can be applied to individual firewalls or across all firewalls.



Top Blocked Websites

	Website	Category	%	Visits	Total: 1626
1.	finance.yahoo.com	Finance and Banking	5.8%	95	
2.	yahoo.com	Search Engines	5.8%	94	
3.	mail.yahoo.com	Web-based Email	5.8%	94	
4.	sports.yahoo.com	Sports	5.5%	89	
5.	biz.yahoo.com	Business	5.3%	86	
6.	www.adware.com	Advertising	5.1%	83	
7.	mail.hotmail.com	Web-based Email	4.7%	77	
8.	download.com	Pay to Surf	4.7%	77	
9.	www.bseindia.com	Finance and Banking	4.6%	74	
10.	bizlive.com	Business	4.5%	73	
11.	Other (13)		48.2%	784	

Figure 4: Web application usage reports

Application monitoring and reporting

The application monitoring and reporting feature collects application traffic information and displays it using visual trend charts. This provides administrators with a quick way to gain insight into application usage on their network. Administrators can select from several different types of charts to display data graphically. Default chart types include; top Web categories, top blocked Websites, top ten applications by bandwidth, top ten media users by bandwidth, and top users by browse time. Trend charts are generated for each firewall policy that has application monitoring enabled. Using knowledge gained from application trend charts, administrators can optimize the use of applications with simultaneous consideration for their organization's security and for worker access needs.

Application control packet logging

Fortinet Application Control packet logging saves network packets generated by applications for additional analysis, such as forensic investigation or identification of false positives. FortiGate consolidated security appliances can store the packets or forward them on to a FortiAnalyzer unit or even to the FortiGuard Analysis and Management Service.

Application control at the endpoint

FortiClient™ Endpoint Security and FortiMobile™ Smartphone Security are client-based software solutions designed to provide security features for enterprise computers and mobile devices. When used with FortiGate appliances or even as standalone solutions, they provide a comprehensive suite of threat protections for network endpoints. Administrators can create and deploy an application control list at a FortiGate consolidated security gateway, and simultaneously apply that list to the Fortinet Endpoint Security profile. The application control list determines which applications are allowed, monitored, or blocked at the gateway and at the endpoint. The list of available categories, vendors and applications is sent from the FortiGuard signature database. In addition, application use at endpoints can be controlled with a personal firewall.

Online resources

Fortinet offers multiple online resources to compliment Fortinet Application Control. The FortiGuard Application Control List provides detailed information about all applications listed in the FortiGuard Application Control Database. The FortiGuard Application Control Site lists the top 10 applications currently in use by Fortinet customers. In addition, customers can easily request new application control signatures and updates by completing an Application Control Submission Form.

Conclusion

Organizations can no longer afford to ignore the use of web-based applications in their network environments. Employees, partners and contractors will continue to demand access to Web 2.0 applications in order to stay connected and maintain productivity which can, in turn, increase network traffic and threat levels.

A security solution that provides complete content protection including application detection, monitoring and control is needed to discover threats embedded in Internet-based application traffic, and to protect against data loss resulting from inappropriate use of web-based social media applications. In addition, content-based security enforcement is essential to mitigate these threats when they are discovered and to provide compete protection and threat elimination. FortiOS provides these multiple levels of threat protection when Fortinet Application Control is combined with FortiOS UTM features such as intrusion prevention, antivirus/antispyware protection and data loss prevention.

To learn more about Fortinet Application Control and the FortiGuard Application Control database, please visit Fortinet at:

http://www.fortiguard.com/applicationcontrol/appcontrol.html

About Fortinet

Fortinet delivers unified threat management and specialized security solutions that block today's sophisticated threats. Our consolidated architecture enables our customers to deploy fully integrated security technologies in a single device, delivering increased performance, improved protection, and reduced costs. Purpose-built hardware and software provide the high performance and complete content protection our customers need to stay abreast of a constantly evolving threat landscape. Our customers rely on Fortinet to protect their constantly evolving networks in every industry and region in the world. They deploy a robust defense-in-depth strategy that improves their security posture, simplifies their security infrastructure, and reduces their overall cost of ownership.

About FortiOS

FortiOS is a security-hardened, purpose-built operating system that is the software foundation of FortiGate multi-threat security platforms. FortiOS software enables high performance multi-threat security by leveraging the hardware acceleration provided by FortiASIC™ content and network processors. This combination of custom hardware and software gives you the best security and performance possible from a single device. FortiOS helps you stop the latest, most sophisticated, and dynamic threats facing your network today with expert threat intelligence delivered via FortiGuard® Security Subscription Services.

FortiOS 4.0 software redefines network security by extending the scope of integrated security and networking capabilities within the FortiGate multi-threat security platform. Regardless of the size of your organization, you can benefit from the most comprehensive suite of security and networking services within a single device on the market today.

FortiGuard® Security Subscription Services deliver dynamic, automated updates for Fortinet products. The Fortinet Global Security Research Team creates these updates to ensure up-to-date protection against sophisticated threats. Subscriptions include antivirus, intrusion prevention, web filtering, antispam, vulnerability and compliance management, application control, and database security services.

FortiCare™ Support Services provide global support for all Fortinet products and services. FortiCare support enables your Fortinet products to perform optimally. Support plans start with 8x5 Enhanced Support with "return and replace" hardware replacement or 24x7 Comprehensive Support with advanced replacement. Options include Premium Support, Premium RMA, and Professional Services. All hardware products include a 1-year limited hardware warranty and 90-day limited software warranty.

GLOBAL HEADQUARTERS
Fortinet Incorporated
1090 Kifer Road, Sunnyvale, CA 94086 USA
Tel +1.408.235.7700
Fax +1.408.235.7737
www.fortinet.com/sales

EMEA SALES OFFICE – FRANCE
Fortinet Incorporated
120 rue Albert Caquot
06560, Sophia Antipolis, France
Tel +33.4.8987.0510
Fax +33.4.8987.0501

APAC SALES OFFICE – SINGAPORE
Fortinet Incorporated
300 Beach Road #20-01
The Concourse, Singapore 199555
Tel: +65-6513-3734
Fax: +65-6295-0015