



THE IMPORTANCE OF WEB CONTENT FILTERING

FORTINETTM
REAL TIME NETWORK PROTECTION

www.fortinet.com

Contents:

THE PROBLEM	PAGE 3
A NEW GENERATION OF WEB-BASED THREATS	PAGE 4
PHISHING FOR INFORMATION	PAGE 5
BLENDED NETWORK THREATS RISING	PAGE 7
FILE SHARING APPLICATIONS TESTING CORPORATE USAGE POLICIES	PAGE 7
WEB SITES USED FOR ATTACKS	PAGE 8
THE NEED TO MONITOR AND CONTROL WEB ACCESS	PAGE 9
THE DIFFERENT WAYS OF CONTROLLING ACCESS	PAGE 11
FORTINET'S MULTI-FUNCTION SECURITY APPROACH	PAGE 13
HOW FORTIGUARD WORKS	PAGE 14
THE FORTINET ADVANTAGE	PAGE 17
ABOUT FORTINET (WWW.FORTINET.COM)	PAGE 19

>> *Productivity, accessibility and conveniences of the World Wide Web have spurred network-borne viruses, worms, trojans, identity theft, and Internet scams*

THE PROBLEM

The World Wide Web (WWW) has become a critical and integral part of modern business communications as well as a national pastime for billions of users. With millions of applications and world wide access to information, email, video, music, instant messaging (IM), voice-over-ip (VoIP), etc. the way we conduct business, communicate, shop, and entertain is changing rapidly. With all of the good attributes of increased communications and productivity, comes an ugly underside fraught with security risks. Productivity, accessibility and conveniences of the World Wide Web have spurred network-borne viruses, worms, trojans, identity theft, and Internet scams. These are among the increasing risks associated with simple WWW access that was once taken for granted only a few years ago.

Undoubtedly, surfing the Web is the most common of all Internet applications. It offers global access to nearly any type of information, allows the purchasing of goods and services from the comfort of our computer, and entertains in many different ways. For business, it has been a productivity tool as well as a new challenge. Some of the negative impacts of the World Wide Web include:

- Lost productivity due to non-business related internet use
- Legal liability due to offensive behavior with inappropriate content
- Higher costs as additional bandwidth is purchased to support legitimate and illegitimate business applications
- Exposes sensitive corporate information through instant messaging, non-approved email accounts, spyware, backdoor trojans, etc.
- Infection and destruction of corporate information and computing resources due to non-business related internet access

For both businesses and individuals, the web has unfortunately become the new breeding ground for malicious activity. It's standards-based world wide appeal and incredible number of applications has made it the medium of choice for modern hackers and thieves looking for new ways to disrupt services, steal information, and perform malicious activities for financial gain. Corrupting user's computers, or worse, stealing personal data through web-borne viruses, worms and Trojan applications is becoming increasingly common.

The number of identity thefts is on the rise and theft of credit card information, fraud, etc has increased dramatically. The need for complete content security is rising quickly as corporations are quickly realizing that traditional security devices such as firewalls, IDS, and host based Antivirus are no longer protecting them from the new generation of threats. Reports from IDC show that the rise in the Secure Content Management (SCM) appliances (Antivirus, Web Content Filtering, and Messaging Security) has increased significantly since 2002. With annual revenues from SCM vendors growing from \$4.2 billion in 2004 to \$7.5 billion in 2008 - a 16.0% compound annual growth rate (CAGR) from 2003 to 2008.

>> As government regulations and legal requirements begin to hold company executives accountable for their employee's actions, corporate executives and IT professionals alike are now becoming more concerned about what their employees are viewing and downloading from the Internet

Not only is the number and severity of threats increasing on the outside of your network, but the potential for damage is increasing inside the corporate walls as well. Casual non-business related web surfing has caused many businesses countless hours of legal litigation, as hostile work environments have been created by employees who view and download offensive content. Copyright infringement lawsuits filed by the music and movie picture industries are increasing as employees use file-sharing programs to download their favorite music and movie files. As government regulations and legal requirements begin to hold company executives accountable for their employee's actions, corporate executives and IT professionals alike are now becoming more concerned about what their employees are viewing and downloading from the Internet.

To address network and web based threats, Fortinet offers several technologies to help customers secure their corporate networks. FortiGuard Web Content Filtering service along with its traditional web filtering technologies offer a wide variety of protection including web content analysis based on banned words, URL blocking, and automated category blocking. The FortiGuard service, described in greater detail towards the end of this application note, has established a ratings database of more than 15 million domains made up of 56 known categories to provide fast efficient protection against web based threats and unauthorized access to non-business related web sites.

Fortinet's FortiGate Antivirus Firewalls don't stop at just web content filtering either. With its stateful firewall, network based antivirus, intrusion detection and prevention system (IDS & IPS), IPSec VPN, Anti-Spam filtering, and bandwidth shaping capabilities in addition to web content filtering, Fortinet security platforms provide the world's most feature rich security appliance. Combined with ASIC accelerated performance and its Dynamic Threat Prevention System, FortiGate Antivirus Firewalls provide protection against network based security threats at all application layers and raises the bar in detecting known and unknown threats.

A NEW GENERATION OF WEB-BASED THREATS

The types of web-based attacks and threats are not only increasing year-over-year, but they are getting much more sophisticated - using technology as well as social engineering to trick users into executing the malicious payload and exposing their systems and/or personal information. New threats and web-based applications that are causing additional problems to many corporate networks include:

- Spyware (also known as Grayware)
- Phishing
- Instant Messaging
- Peer-to-Peer File Sharing
- Streaming Media
- Blended Network Attacks

>> *Phishing attacks use Web sites and emails that claim to be from legitimate banks, e-commerce sites, investment firms and other financial organizations to lure their victims into believing the message is legitimate*

Two of the latest forms of Web based threats that are rapidly gaining media attention are Phishing and Spyware / Grayware.

PHISHING FOR INFORMATION

Phishing is the term used to describe social engineering attacks that use email and web technology to trick users into giving out personal or financial information to the attackers. Phishing attacks use Web sites and emails that claim to be from legitimate banks, e-commerce sites, investment firms and other financial organizations to lure their victims into believing the message is legitimate. Nearly always, the email will request that the user verify their personal information (social security numbers, account ID, passwords, credit card information, etc.) to continue service or prevent disruption of existing services.



Figure 1: Phishing Example #1

Although Phishing is initiated by spam email, getting the user to access the attacker's web site to provide personal information is always the next step. Examples of Phishing are illustrated in the following examples.

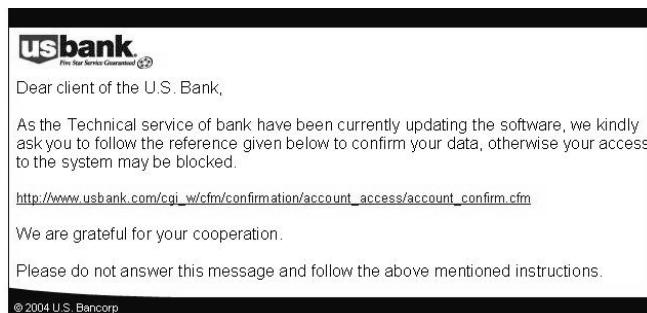


Figure 2: Phishing Example #2

Customers can use different technologies to start detecting and blocking Phishing attempts. Tuning their anti-spam solutions to block Phishing spam is the 1st step. Using web content filtering to detect and block Phishing web sites is the 2nd step. Educating employees and constantly reminding them of the dangers of Phishing is the 3rd step. By combining all of these methods, corporations can reduce the potential threat and exposure to Phishing attacks.

DANGEROUS & STEALTHY GRAYWARE/SPYWARE

Grayware is an umbrella term applied to a wide range of applications that are installed on a user's computer to track and/or report certain information back to some external source. These applications are usually installed unknowingly and run without the permission of the user. Some forms of grayware come as Trojan applications that trick users into installing them, while others are installed through browsing spyware infected web sites. The fact is that spyware and grayware can come from any number of places and activities, including Phishing sites. Some of the most common ways of grayware infection include:

- Downloading shareware, freeware, or other forms of file sharing services
- Opening infected emails
- Clicking on pop-up advertising
- Visiting frivolous or spoofed web sites
- Installing Trojan applications
- Visiting legitimate compromised web sites infected with grayware

The most common categories of Grayware include:

- Spyware
- Adware
- Keystroke Loggers
- Dialers
- Web Page Hijacker
- Toolbar Editors
- Browser Helper Objects
- Download Programs
- Remote Administration Tools
- Network Management
- Browser Plugins
- Games
- Jokes
- Peer2Peer

With the advent of this new threat, the word "Spyware" is becoming well known in IT and security circles and has drawn significant media coverage. End users are now becoming aware of the potential threats and are realizing just how stealthy these applications can be.

Spyware has become a serious and dangerous problem for all computer users alike. So serious that the US Government's House of Representatives passed two bills in October 2004 to enforce and penalize abusers of spyware and Phishing spam - the "Internet Spyware Prevention Act (H.R. 4661)" and the "Spy Act (H.R. 2929)".

Some of the threats introduced by spyware include:

- Tracking Internet usage patterns and reporting them back to the attacker
- Tracking key strokes for usernames, passwords, credit card information, etc.
- Grooming hard drives for specific information

>> Attackers are learning from each previous successful attack and are enhancing and updating attack code to become more dangerous and fast spreading.

- Reading and monitoring cookie usage
- Redirection to other web sites
- Addition of toolbar applications
- Installing malicious programs
- Using modems to make premium 900 calls
- Turning on microphones and webcams for spying
- Slowing down or crashing computers

By combining Grayware/Spyware AV inspection with Web Content Filtering, corporations can significantly reduce the exposure and threats introduced by Grayware. Fortinet's FortiGuard Web Content Filtering service has over 28,500 spyware sites defined and can be used to significantly reduce the risk of exposure to spyware sites.

BLENDED NETWORK THREATS RISING

The sophistication of network threats is increasing with each new attack. Attackers are learning from each previous successful attack and are enhancing and updating attack code to become more dangerous and fast spreading. Blended attacks use a combination of attack methods to spread and cause damage. Using virus or network worm techniques combined with known system vulnerabilities, blended threats can quickly spread through email, web sites, and Trojan applications. Examples of recent blended attacks include Nimda, Code Red, Slammer, and Blaster. Blended attacks can be designed to perform different types of attacks - from disrupting network services to destroying or stealing information to installing stealthy backdoor applications to grant remote access.

The success of blended threats are proving that traditional stateful firewalls, signature based antivirus, and intrusion detection systems are not enough. Security systems will have to incorporate much more sophisticated heuristic and anomaly detection methods to increase the detection rate of new "zero hour" attacks.

FILE SHARING APPLICATIONS TESTING CORPORATE USAGE POLICIES

With the popularity of peer-to-peer file sharing, video and music downloads, and instant messaging, many companies are facing new challenges that they never had to address before. Peer-to-peer file sharing applications are changing the way people share information and that's both good and bad. One of the negative impacts of peer-to-peer applications is controlling how sensitive company information is sent and received by employees, where the data is stored outside the company, and how secure the peering server is from prying eyes.

In addition to peer-to-peer file sharing applications, there are numerous programs designed to download and exchange music and movie files. This not

>> The challenges of keeping users satisfied and safeguarding corporate assets is becoming a daunting task for IT and Security professionals alike.

only takes up valuable network resources and lowers employee productivity, but it also brings legal implications with the copyright laws that are associated with music and movie files. Music and movie companies are now actively pursuing and prosecuting businesses, educational institutions, and individuals who freely copy music and movies - and they are winning against the violators. Unknown to many users of these file sharing applications, is the fact that many of the specialized music download programs are also littered with spyware applications used to track and report Internet usage patterns.

Peer-to-peer file sharing and download applications can also be used to expose company trade secrets, corporate non-public information, and other sensitive information and bring legal issues and negative PR. With Instant Messaging (IM), user productivity and control of sensitive information are affected. Sensitive information may be transmitted in the clear over the Internet and stored on servers that are not controlled and secured in accordance with the company's computer security policies. The other downside is lost productivity as employees spend time "chatting" with friends and family members during work hours.

WEB SITES USED FOR ATTACKS

With the successful attack of JS/Scob (also known as Download.Ject) and the IMBIG Trojan in the summer of 2004, the level of attack sophistication was raised again. With JS/Scob, vulnerable web sites were broken into and infected with a series of malicious software which in turn infected user's computer systems when they visited the infected web site. JS/Scob installed several backdoor applications and a keystroke logger that allowed the attackers to steal personal information from the user's PC. The malicious programs were designed to capture and report personal information when visitors used financial web services - such as banks, investment brokerage sites, etc.

Driven by financial gain, these types of attacks are extremely dangerous to all users conducting financial transactions on the Internet. With their stealthy nature, no signs of malicious activity are displayed on the user's systems and can remain undetected for weeks and months - trapping unsuspecting users into divulging their sensitive personal information.

With faster Internet access and new web-based applications, comes a new generation of vulnerabilities and threats leveraging these advancements. The challenges of keeping users satisfied and safeguarding corporate assets is becoming a daunting task for IT and Security professionals alike. The exposure to modern vulnerabilities is accelerating as threats become more sophisticated and security vendors are rushing to fill the void. Data security must now evolve into a multi-faceted approach and be implemented at all aspects of the network - perimeter, DMZ, core, and endpoints. The need to scan, inspect, monitor and control access has become clearer than ever.

THE NEED TO MONITOR AND CONTROL WEB ACCESS

The instant accessibility to information has been a blessing and source of pain for all types of businesses as well as home users. Traditional firewalls, intrusion detection systems, and antivirus solutions that are commonly used to secure the modern enterprise can not help in the areas of monitoring and securing web surfing activities conducted by employees. With the popularity of using more and more Web applications along with the reasons mentioned previously, the need to monitor and control Web access is becoming clearer to all businesses large and small.

IDC reports that the growth in WEB Content Filtering will grow over the next five years (2003 - 2008) at a Compound Annual Growth Rate (CAGR) of 22.6% and become a key component of Secure Content Management systems (SCM) which employ antivirus, web filtering, and messaging security.

Popular reasons for web content inspection and filtering include:

- Lost productivity when employees are accessing the Web for non-business reasons.
- Network congestion - valuable bandwidth is being used for non-business purposes and legitimate business applications suffer.
- Increasing costs as more Internet bandwidth is added to support both legitimate and illegitimate business applications.
- Loss or exposure of confidential information through chat sites, non-approved email systems, Instant Messaging, peer-to-peer file sharing, etc.
- Increased exposure to web-based threats (viruses, worms, trojans, spyware, etc.) as employees surf non-business related web sites.
- Legal liability when employees accesses inappropriate and offensive material (pornography, racism, etc).
- Copyright infringement caused by employees downloading and/or distributing copyrighted material such as music, movies, etc.
- Negative publicity due to exposure of critical company information, legal action, etc.
- Worldwide government regulations on Internet access and information security are being enforced by many countries and individual states:
 - Children's Internet Protection Act (CIPA) for schools and libraries
 - Japan's Internet Association introduced "SafetyOnline2" to promote internet filtering HIPPA
 - Sarbanes-Oxley
 - Gramm-Leach-Bliley
 - Privacy and 'Duty of Care' legislation
- The need to enforce corporate Internet Usage Policies require the ability to monitor and block unauthorized web sites.

Many independent reports and government agencies (such as the FBI) are now showing that employees are becoming the single highest risk and most common cause of network abuse, data loss and legal action. Because employers can be ultimately held responsible for their employee's actions, many businesses are now working aggressively with their Human Resources departments to define what acceptable Internet usage is.

Industry analysts' reports of Internet abuse include:

- IDC reports that 30 - 40% of internet access is being used for non-business purposes.
- The American Management Association reports that 27% of Fortune 500 companies have been involved in sexual harassment lawsuits over their employee's inappropriate use of email and Internet use.
- The Center of Internet Studies have reported that more than 60% of companies have disciplined employees over Internet and email use with more than 30% terminating employees.
- Numerous stories of employee dismissal, sexual harassment, and discipline with regards to Internet use can be found on the Internet:

http://www.theregister.co.uk/1999/06/16/it_manager_fired_for_lunchtime

http://www.theregister.co.uk/2000/07/15/xerox_fires_40_in_porn

<http://www.internetweek.com/lead/lead101599.htm>

- The Recording Industry Association of America (RIAA) and the Motion Picture Association of America (MPAA) have pursued legal action against corporations over the illegal downloading of music and movies from the Internet. The RIAA recently won a case against an Arizona company for \$1 million dollars.
- A big oil and gas company recently paid \$2.2 million dollars to settle a lawsuit for tolerating a hostile work environment created by the downloading of Internet pornography.

To address the issues mentioned previously, companies are creating or updating their computer usage policies to include web, email, and general Internet usage in order to protect themselves from legal action. In order to become compliant with many of these new policies, corporations need to start monitoring and controlling web access. Web content filtering is gaining popularity and the industry providing the tools and technology in this area have been growing rapidly - IDC has predicted a compound annual growth rate of 27% year-over-year until 2007.

>> There are several different technologies that help facilitate web monitoring, logging and filtering

THE DIFFERENT WAYS OF CONTROLLING ACCESS

The methods available for monitoring and controlling Internet access ranges from manual and educational methods to fully automated systems designed to scan, inspect, rate, and control web activity. Common web access control mechanisms include:

- Establishing a well written usage policy
- Communicating the usage policy to every person in the organization
- Educating everyone on proper Internet, email, and computer conduct
- Installing monitoring tools that record and report on Internet usage
- Implementing Policy Based tools that capture, rate, and block URLs
- Taking appropriate action when complaints are registered, policies violated, etc.

TECHNOLOGY FOR WEB CONTENT FILTERING

There are several different technologies that help facilitate web monitoring, logging and filtering of http, ftp, and other web related traffic. Many solutions are software based and run on Intel based servers that are attached to the network through a "mirrored" network port. Other solutions are dedicated appliances that are installed inline with the network, allowing it to see all of the Internet traffic and allowing it to take fast responsive action against non-authorized and malicious content.

Some of the most common methods for web content filtering include:
Banned Word List

- This method allows the creation of a "black List" dictionary that contains words or phrases. URLs and web content is compared against the black list to block unauthorized web sites. In the beginning, this technology was largely a manual process with vendors providing black lists as starting points, requiring customers to manually update/tune the lists by adding or excluding key words. This method has improved over the years and vendor lists have grown to include millions of key words and phrases. Updates are usually performed manually and filtering accuracy may be impacted with specific categories. For example, medical research sites are often blocked as they are mistaken for offensive material.

URL Block

- The URL Block is a "black list" containing known bad or unauthorized web site URLs. Entire URLs can be added to the black list and exemptions can usually be made to allow portions of the web site through. Many vendors provide URL black lists with their products to simplify the technology, giving the user the ability to add new sites and perform URL pattern matching. With both Banned Word lists and URL Block lists, the customer must perform manual updates of the vendor's black lists. Depending on the frequency of the updates, the black lists may fall out of compliancy with the corporate policy in between updates.

>> *The need to react in real-time with web content filtering is becoming increasingly important in network security*

Category Block

- Category Blocking is the latest web content filtering technology that greatly simplifies the management process of web inspection and content filtering. Category Blocking utilizes external services that help keep suspect web sites up-to-date - relying on Web Category Servers that contain the latest web URL ratings to perform web filtering. With Category Blocking devices, there are no manual lists to install or maintain. Web traffic is inspected against rating databases installed on the Category Servers and the results (good or bad sites) are cached to increase performance. The advantage is up-to-date web URL and category information at all times, eliminating the need to manually manage and update local black lists. This method ensures accuracy and real-time compliance with the company's Internet Usage Policy.

Just like Antivirus and Intrusion Protection Systems, the need to react in real-time with web content filtering is becoming increasingly important in network security. Network worms that spread globally within hours (Slammer, Blaster, Welchia, etc) have been experienced by nearly all corporations over the last few years. The ability to react accurately to unauthorized web content is becoming just as critical as more and more attacks are disguising themselves as innocent email and web page URLs.

Many new threats such as spyware and Phishing are combinations of spam email and dangerous web URLs that need to be stopped at the network perimeter - before they can enter the corporate network and fool employees into executing the attack. Through multi-functional security devices such as Fortinet's FortiGate security platforms, customers can increase the detection rate and provide better protection against blended threats. By having antivirus, IDS & IPS, as well as web content filtering and anti-spam with the ability to receive automated signature and web URL rating updates, the bar is significantly raised against threats and attacks designed to fool single function security systems.

IDC reports that the worldwide revenue for Secure Content Management (SCM) Services is growing quickly as corporations realize the benefits of security services - easy of deployment, management, and updates. From the past few rapid spreading network attacks, many IT professionals have realized that the manual updating of antivirus signatures, web content ratings, and spam information is becoming too slow to be really effective against the latest rapid spreading threats. IDC's July 2004 report on the SCM Services Market shows a 56% growth from 2002 to 2003 with the growth of SCM devices growing at a 54.4% CAGR from 2003 to 2008.

With legal liability and law suits becoming more frequent, corporations are upgrading to modern SCM systems for antivirus, web content filtering, and

>> *Fortinet has developed the worlds first Dynamic Threat Prevention System*

anti-spam to regain user productivity, reduce liability, reduce maintenance overhead, enforce Internet user policies, and comply with new government requirements.

FORTINET'S MULTI-FUNCTION SECURITY APPROACH

Fortinet's unique approach to protecting networks against the latest vulnerabilities involves several key security components. By combining seven key security functions into one ASIC accelerated security hardware and software platform, Fortinet has developed the worlds first Dynamic Threat Prevention System. By sharing information between each component and relying on powerful firewall and IPS capabilities, threats are identified quickly and proactively blocked at the network level before they reach the endpoints to cause damage. Customers can create custom Protection Policies by turning on any of the seven security functions in any combination and applying them to the interfaces on the FortiGate Antivirus Firewall platforms - Stateful Firewall, IPSec VPN, Antivirus, IDS & IPS, Web Content Filtering, Anti-Spam, and Bandwidth Shaping.

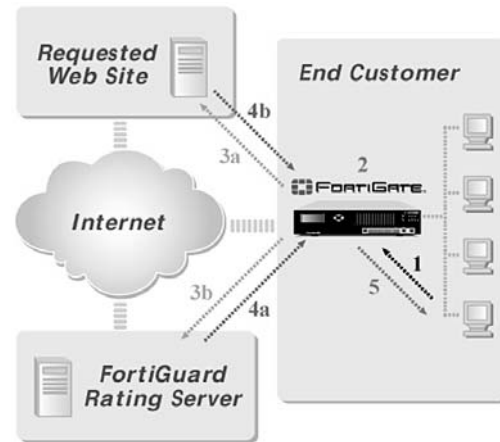
Fortinet's Web Content Filtering technology allows customers to take a wide variety of actions to inspect, rate, and control web traffic. Included with each FortiGate security platform is the ability to control web traffic via:

- Banned Word Lists
- Wildcard Pattern Matching
- Multi-Language Pattern Matching
- URL Block Lists
- Web Pattern Lists
- URL Exemption Lists
- Web Application Block (Java Applet, Cookie, ActiveX)
- Category Block (via FortiGuard Service)

Customers can mix and match any of the web content filtering methods to achieve the correct balance for enforcement or select Fortinet's Automated Category Blocking option - FortiGuard Web Filtering Solution. By combining Fortinet's Web Content Filtering system with its Antivirus, IDS & IPS, and Anti-Spam functions, the success rate of detecting and blocking new blended threats is increased many times over a single function security device or service.

HOW FORTIGUARD WORKS

Fortinet's FortiGuard Web Filtering solution is a hosted service designed to provide Web URL filtering for schools, libraries, government agencies, and enterprise businesses of all sizes. FortiGuard Web Filtering solution consists of



two parts, the FortiGuard Rating Server and the FortiGate multi-function security platform. The FortiGuard Rating Server is a master ratings database that is made up of over 15 million domains and several billion web pages, sorted into 56 categories.

The FortiGuard Web Filtering solution does not require any additional hardware and can be activated on all FortiGate Antivirus Firewalls.

Figure 3: FortiGuard Overview

1. User requests a URL.
2. If the rating for the URL is already cached in the FortiGate unit, it is immediately compared with the policy for the user. If the site is allowed, the page is requested (3a) and the response is retrieved (4b).
3. If the URL rating is not in the FortiGate cache, the page is requested (3a) and a rating request is made simultaneously to the FortiGuard Rating Server (3b).
4. When the rating response is received by the FortiGate unit (4a), it is compared with the requestor's policy (2). The response from the Web site (4b) is queued by the FortiGate unit if necessary until the rating is received.
5. If the policy is to allow the page, the Web site response (4b) is passed to the requestor (5). Otherwise, a user-definable "blocked" message is sent to the requestor and the event is logged in the content filtering log.

The heart of the FortiGuard system is the FortiGuard Rating Database that contains over 15 million domains and over several billion rated web pages. Thousands-upon-thousands of new submissions are added or updated daily to keep the web rating information up-to-date. FortiGuard Rating Servers are distributed world wide to provide reliable uninterrupted service to all FortiGate security platforms deployed around the globe. The Rating Databases are updated continuously every day to provide real-time protection against suspect, unauthorized, and dangerous web sites as they are discovered. There is no need for customer interaction or manual updating of critical databases to obtain the latest protection against new malicious web-based threats.

FORTIGUARD WEB CATEGORIES

FortiGuard's web content filtering service is a technology leader in rating accuracy and the breadth of its content categories. With over 15 million rated domains and several billion rated web pages, FortiGuard accurately scans, rates, and filters web traffic against the following categories:

1. Abused Drugs	20. Games	39. Reference Materials
2. Cult or Occult	21. Internet Communication	40. Religion
3. Hacking	22. Pay to Surf	41. Search Engines & Portals
4. Illegal or Questionable	23. Web-based Email	42. Shopping and Auction
5. Racism or Hate	24. File Sharing and Storage	43. Social Organizations
6. Violence	25. Streaming Media	44. Society and Lifestyles
7. Abortion	26. Malicious Web Sites	45. Special Events
8. Adult Materials	27. Spyware	46. Sports
9. Advocacy Groups	28. Arts and Entertainment	47. Travel
10. Alcohol and Tobacco	29. Cultural Institutions	48. Vehicles
11. Gambling	30. Education	49. Business and Economy
12. Militancy and Extremist	31. Financial Data & Svcs	50. Computer Security
13. Nudity Organizations	32. Gay/Lesbian/Bisexual	51. Government and Legal
14. Pornography	33. Health	52. Information Technology
15. Tasteless	34. Job Search	53. Military Organizations
16. Weapons	35. Medicine	54. Dynamic Content
17. Advertisement	36. News and Media	55. Miscellaneous
18. Brokerage and Trading	37. Personals and Dating	56. Web Hosting
19. Software Download	38. Political Organizations	

Table 1: FortiGuard Category Distribution Table

SIMPLE SETUP AND MAINTENANCE

With FortiGuard, users can maintain complete control over their web content filtering services from one central console. Web filtering is enabled on each firewall policy and is fully configurable through an intuitive web user interface. Web content filtering can also be combined with any of the other Fortinet security functions to provide superior detection and threat prevention against the latest known and unknown attacks. For example, customers can combine antivirus, anti-spam, and web content filtering into one Protection Policy to be deployed on a particular interface.

The 56 categories are summarized into 8 general categories and customers can decide to allow, block, or monitor access to these types of web sites. Each summarized category can be expanded and each of the 56 categories can be configured with a different policy action.

>> Track accountability
and provide detailed
reporting on every
security aspect

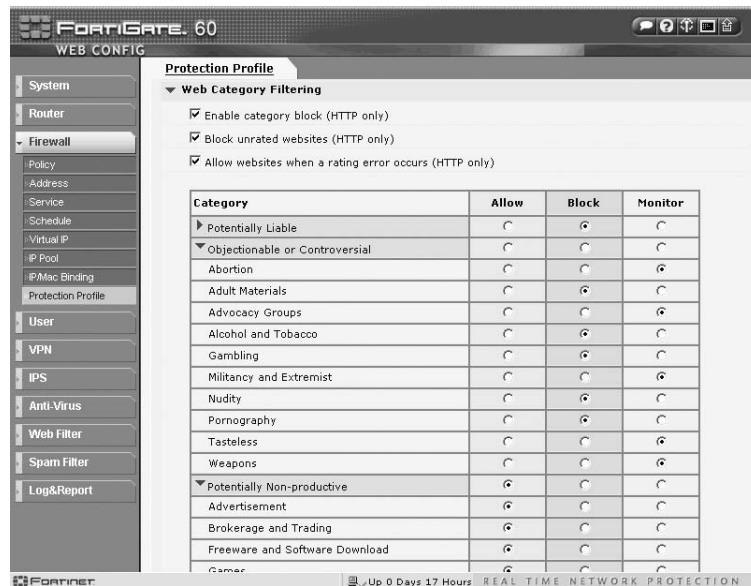


Figure 4: FortiGuard Web Category Filtering Protection Profile

ACCOUNTABILITY AND REPORTING

FortiGuard security platforms allow a wide array of internal and external reporting features to track accountability and provide detailed reporting on every security aspect the system provides. With FortiGuard logging enabled, the following information is captured:

- Source IP
- Destination IP
- URL
- Policy Action (allow, block, monitor)
- Content Category

Through authentication profiles, customers can increase tracking and enforceability measures. With authentication enabled, users must authenticate successfully to the FortiGate unit (through a local user database, LDAP, or RADIUS) before gaining access to the Internet. All logged Internet activity is tagged with the associated user's authentication information to provide detailed logging and reporting of employee web surfing activity.

By using Fortinet's external logging and reporting systems, FortiLog or FortiReporter, customers can gain detailed insight into their corporation's Internet activities and regain control of their network resources, improve productivity and reduce the substantial risks and legal liability associated with inappropriate and illegal content.

>> Fortinet developed a high-performance security ASIC (FortiASIC) that is specifically designed to speed up the computationally intensive routines commonly associated with complete content protection

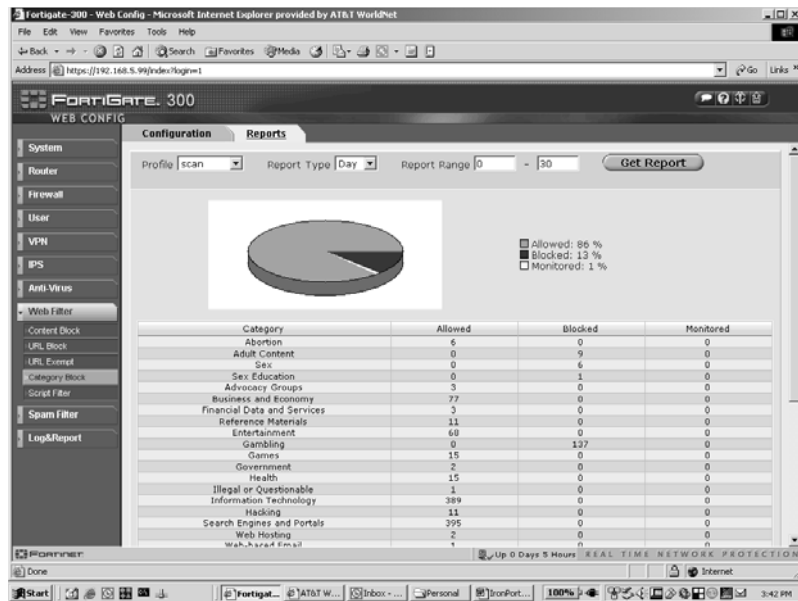


Figure 5: FortiGuard Category Activity Report

THE FORTINET ADVANTAGE

The number of threats and vulnerabilities are continuing to grow and the need to stay on top of operating system patches, application patches, antivirus signatures, and so forth are becoming more critical and difficult to do. The need for Web Content Filtering is just one of the areas that business customers are looking to solve. Fortinet solves this security problem along with many others using its award winning FortiGate security platforms by providing a Dynamic Threat Prevention System to detect, remove, and block both known and unknown threats and anomalies.

To create this multi-tiered security system without major performance penalties, Fortinet developed a high-performance security ASIC (FortiASIC) that is specifically designed to speed up the computationally intensive routines commonly associated with complete content protection, which goes beyond Deep Packet Inspection and performs real-time content reassembly and analysis. This unique approach delivers performance for antivirus, grayware, IDS, encryption, content analysis, and related functions that is increased significantly over software-based security applications - and at a much lower cost.

To provide solid inspection, detection and prevention services, FortiGate units are ICSA Labs certified for Firewall, Antivirus, Intrusion Detection & Prevention, and IPSec VPN. The dedicated hardened FortiOS™ operating system provides real-time, high-performance, robust and reliable network security that can be applied at the network perimeter as well as into the network core. There are over a dozen FortiGate models starting with compact, low-cost devices to support telecommuter and SOHO applications and scaling to address high-performance, non-stop applications in the service provider core. To extend Fortinet's security to mobile users when they are not in the office,

Fortinet's FortiClient software provides a well-rounded set of security applications to protect all corporate assets on the PC. FortiClient v1.2 provides Virtual Private Network, Personal Firewall, Antivirus, and Spyware/Grayware protection to help keep unwanted traffic out.

To keep the security components up-to-date, Fortinet provides the FortiProtect Network to automatically update every FortiGuard unit when new security threats are identified - in real-time! Unlike traditional security solutions that require manual updating, the FortiProtect Network updates the FortiGuard security signatures as new threats become known - greatly decreasing the likelihood of being attacked by new security threats.

Coupled with Fortinet's central management, reporting, logging systems and FortiProtect updates, enterprises can feel confident when implementing grayware security solutions from Fortinet. With Fortinet's simple licensing scheme that avoids per-user or per-seat licenses, the cost of implementing a world-class enterprise security system is much lower than competitive solutions.

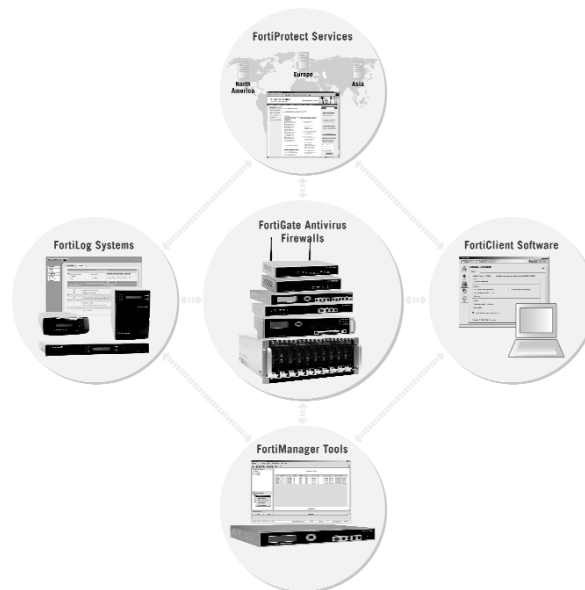


Figure 6: Unified Threat Management System

Fortinet products have won numerous awards including the 2003 Networking Industry Awards Firewall Product of the Year and the 2004 Security Product of the Year Award from Network Computing Magazine. In September 2004, IDC named Fortinet as the leader (with 29.5% market share) in their new Unified Threat Management (UTM) security category. UTM is one of the fastest growing segments in the security space with sales of UTM products projected to surpass that of traditional Firewall and VPN appliances by 2008.

[HTTP://FORTINET.COM/PRODUCTS/FORTIGUARD.HTML](http://fortinet.com/products/fortiguard.html)

ABOUT FORTINET (WWW.FORTINET.COM)

Fortinet is the confirmed leader of the Unified Threat Management market. The company's award-winning FortiGate™ series of ASIC-accelerated antivirus firewalls, winner of the 2004 Security Product of the Year Award from Network Computing and the 2003 Networking Industry Awards Firewall Product of the Year, are the new generation of real-time network protection systems. They detect and eliminate the most damaging, content-based threats from e-mail and Web traffic such as viruses, worms, intrusions, inappropriate Web content and more in real time - without degrading network performance. FortiGate systems are the only security products that are quadruple-certified by the ICSA (antivirus, firewall, IPSec, NIDS), and deliver a full range of network-level and application-level services in integrated, easily managed platforms. Named to the Red Herring Top 100 Private Companies, Fortinet is privately held and based in Sunnyvale, California.

FOR MORE INFORMATION

More information about Fortinet, FortiGate Antivirus Firewall products, FortiProtect Center and other services provided by Fortinet is available from the following sources:

SALES

Please contact us at sales@fortinet.com or phone toll-free in the U.S. (866) 868-3678 or +1(408) 235-7700.

POTENTIAL PARTNERS

Please contact us at partners@fortinet.com or visit us at www.fortinet.com.

Copyright 2004 Fortinet, Inc. All rights reserved. Fortinet, FortiGate, FortiClient, FortiGuard, FortiOS, FortiProtect, FortiASIC and ABACAS are registered trademarks of Fortinet Corporation in the United States and/or other countries. The names of actual companies and products mentioned herein may be the trademarks of their respective owners. WPR1120410

