astaro
internet security

Network Security Whitepaper

Effective Web Blocking
A Technology Primer on URL Content Filtering

Version: 2.00
Release date: August 16, 2006

Table of Contents

Emerging Internet Access Issues 3
Managing Internet Usage 3
Web Filtering Technologies 4
Overview Of The Automatic Content Filtering Process 6
Content Acquisition 7
Content Analysis 7
Overall Classification 9
Support for Multiple Languages 9
Implementing A Web Filtering Solution 10
Integrating Web Filtering Into A Security Architecture 10
Astaro Security Gateway 11
Conclusion 12
Appendix A: Astaro Surf Protection URL Database Categories 13

Emerging Internet Access Issues

In a relatively short period of time Internet access has become ubiquitous in most organizations. A side effect of its rapid growth is the fact that many organizations are still grappling with the human implications of the technology. Issues vary depending upon the nature of the organization, but leading concerns include:

- Productivity: 60% of all employees report using the Internet to conduct personal business. Given the lack of verbal and physical queues associated with these activities, managers are struggling to define, monitor and control excessive personal usage. The magnitude of potential productivity losses associated with personal web surfing makes it the most pressing human factors issue facing organizations.
- Legal Liabilities: Web access makes downloading inappropriate material such as pornography, copyrighted music files or hate material simple, but difficult to monitor. Yet organizations are being held legally accountable for such activities. Expensive lawsuits citing hostile work environments or the use of unlicensed material have been widely publicized. The financial implications of lawsuits are of course a concern, but the drain from a focus and public relations perspective can be equally damaging, making this issue a high priority for many organizations.
- Core Values: Some organizations, especially in the non-profit area, are built around strong core values. These organizations are highly interested in ensuring any activities that might explicitly or implicitly undermine their values be either avoided, or flagged for management attention.

While the full impact of ubiquitous Internet access is still evolving, it has become clear to most organizations that unrestrained usage can be highly problematic.

Managing Internet Usage

To deal with these issues, most organizations are moving rapidly to develop Internet Usage Policies. In fact, according to Gartner Group, 79% of large companies surveyed reported having such policies. Establishing an effective policy is relatively straight forward, involving three basic steps:

> Step 1: Monitor and understand Internet usage
> Step 2: Develop, document and disseminate an Acceptable Use Policy
> Step 3: Put in place an enforcement mechanism

Unfortunately many companies tend to focus solely on Step 2. While this is a worthy effort, without understanding existing surfing patterns, the policy established may not deal with important issues. More importantly, without enforcement mechanisms, the policy will be ineffective. In the Gartner study previously cited, only 30% of companies indicated they enforced their policies. Enforcement mechanisms are necessary to drive behavioral change.

Enforcement can be problematic. As discussed above, traditional management monitoring techniques are ineffective with web surfing. For this reason companies that implement enforcement policies have focused on using electronic techniques. The technology to inspect and block network requests is, of course, well established, being utilized by virtually every organization in a variety of different applications (firewalls, etc.). However web/URL filtering presents some unique challenges. Given that over 30 million web domains exist today, with the number and composition of those domains changing hourly, how can one accurately determine whether a particular request violates the Acceptable Use Policy in real-time?

This question is the focus of this paper. In subsequent sections we will review various technology alternatives, and then explore in-depth the technology that Astaro believes is most effective in implementing real-time web filtering solutions.

Web Filtering Technologies

Before discussing differences in web filtering technologies it is useful to have an evaluation framework. There are two primary factors that determine whether a web filter is judged to be effective: accuracy and performance.

Accuracy is the key to effective filtering. If a filter misses web sites that should be blocked according to established criteria, it is underblocking. Underblocking results in ineffective enforcement, defeating the purpose of the solution. Overblocking is the term used for the opposite problem, incorrectly blocking web sites that in fact do not violate any of the established blocking criteria. Overblocking may cause user dissatisfaction and productivity losses.

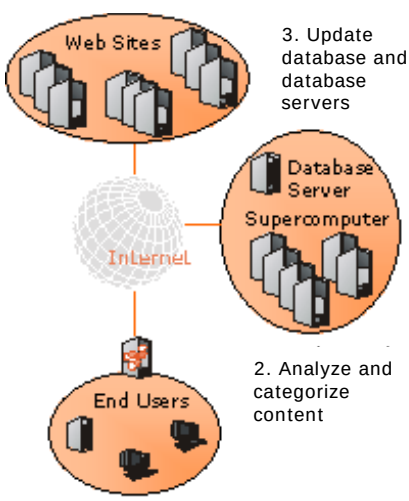
Performance is an absolute requirement for an interactive application such as web filtering. Users accessing the Internet desire near instantaneous response. A filtering solution that introduces noticeable delay will not be tolerated in most organizations.

Two primary categories of web filtering technology exist; dynamic filters and database filters. Dynamic filters examine the contents of web pages as they are requested, to determine if they violate criteria established by the administrator. If they violate the criteria, the request is blocked. The problem with run-time filtering is that accurately analyzing web page content is a very complex process requiring significant CPU power. A dynamic filter may be able to scan for simple key words associated with pornography for instance, but it will not have the capability to identify pornographic images, pornographic text posted as graphic images, or pornography posted in other languages. While some undesirable sites may be blocked by this technology, sophisticated sites designed to evade filters will not. Furthermore, dynamic filters, because of the simplicity of the analytical techniques employed, will also have problems distinguishing between a legitimate medical and pornographic site for instance. Dynamic filters suffer from both excessive under and overblocking. Employing more sophisticated analytical techniques would result in unacceptable performance degradation. As a result, most solutions deployed in real-time business environments use database filtering.

Database filtering employs a different paradigm. When a user requests a web page, the request is compared to a database containing URL's previously classified by web site content category (gambling, hate, pornography, etc.). If accessing that particular category of site is contrary to the organization's Acceptable Use Policy, the request is blocked. This approach is much more successful because the analysis required to categorize the sites is performed off-line. As a result much more sophisticated recognition and categorization techniques can be employed, resulting in both better accuracy and performance.

Overview Of The Automatic Content Filtering Process

Content Filtering Process Used By Astaro Surf Protection



The automatic content filtering process begins with content acquisition. A Supercrawler that is capable of visiting millions of new and updated sites every day constantly and methodically scans the Internet. The content is then analyzed by a supercomputer that uses a sophisticated algorithm combining intelligent text classification with optical image recognition to classify sites into categories. Each day over 100,000 new and modified URL's are visited, and the database is updated with the resulting classifications.

Astaro offers 60 categories of content, which are detailed in Appendix A. These are the categories which users have indicated interest in blocking as part of their Acceptable Use policy. Sites without content in these categories are not listed in the database in order to maximize performance. Categories can be grouped into 18 custom groups to simplify administration.

The categorization process began in 1999. Since that time 60 million top lever URLs have been categorized containing a total of over 3.9 billion web pages and images.

Content Acquisition

In order to acquire content for analysis, a large distributed crawling system that is capable of visiting millions of web servers daily is used. A variety of sources are combined to identify web sites to be visited and analyzed. These including listings in public host lists, domain registry information, hotlinks from other sites, and customer input.

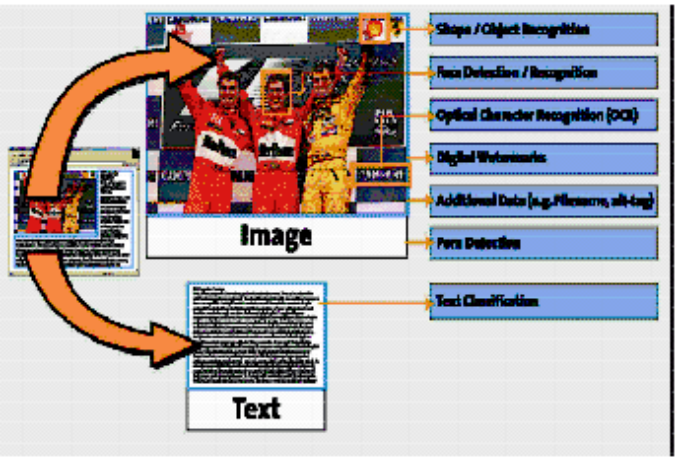
The 500 crawlers in the content acquisition system leverage the tree structure of most sites to maximize coverage and content analysis. Starting at a web site identified for analysis, which forms the root of the tree, the crawler downloads and stores all content (HTML text and images) from that particular site. The crawler then proceeds to follow all hyperlinks (URL's) on the site to additional sites, downloading additional content in the process, until no more unknown hyperlinks exist. To maximize effectiveness, a crawling algorithm has been developed which prioritizes new content discovery. For example, newly discovered hosts and domains are visited before digging deeper into the current host, and downloads are scheduled over multiple visits rather than tying up the crawler with a complete download in a single visit.

In addition to new content discovery, the crawling system is also used to update existing content. Both processes run in parallel, with some of the crawlers searching for new content while others are engaged in updating. Due to the dynamic nature of sites, updating is critical for accuracy. In fact, one technique used to avoid detection by filtering products is to establish a legitimate site, wait for it to be categorized, and then revamp the site with objectionable material. Websites that change more often are crawled more often. At present the crawlers process up to 15 million web pages and images daily and add about 5 million new links every day, once again demonstrating the power of the Astaro approach.

Content Analysis

Once website content has been downloaded by the crawlers, it is classified into categories. As you can see from the adjacent diagram, downloaded content typically consists of multiple data types, each which contains important indicators of the appropriate category.

To minimize over and underblocking, a sophisticated algorithm combining multiple analysis techniques is used on each site. Some of the most important techniques include text classification, visual object



Applying Multiple Content Analysis Technologies

recognition, visual porn detection and optical character recognition. Information from each analysis step contributes to the final classification.

Text Classification

Downloaded text is scanned using two different forms of text analysis, each which has different strengths. Keyword searching uses the occurrence of certain words to categorize content.This method is fast, simple to implement and works well when there is little text to analyze (file names, titles, etc.). On the negative side, many words can be used in different contexts (e.g. sex), making accurate categorization difficult.

Intelligent text classification is the second text analysis method used. This technique considers not only single word occurrence, but also the frequency of occurrence and word combinations. Word heuristics and combinations thereof are used in the final text classification decision process. This technique works best when there are a significant number of words available (whole web sites, etc.). In general, when the number of words is significant, the text classification process is very accurate.

Visual Porn Detection

Objectionable material such as pornography can of course be displayed without significant text descriptors. To help deal with these situations an image analysis technique called visual porn detection that is able to detect high concentrations of flesh tone images is used. Some of the challenges in using this technology are determining which portions of an image are flesh, and whether the flesh portions are appropriate for a non-pornographic image.
To deal with the flesh definition issue, images are scanned to detect faces. If a face is detected, a color sample is taken, allowing accurate detection of flesh in the entire image. If no face is present, statistical assumptions regarding flesh characteristics are used. Face recognition is also used to deal with the flesh proportionality issue. If a face is detected, the size of the head can be determined, allowing the proportion of non-facial flesh to be determined. This allows the algorithm to accurately ascertain when large amounts of flesh are appropriate, as in the case of a facial portrait. The visual porn algorithm has been developed based upon extensive analysis of different images and utilizes a variety of sophisticated analysis techniques to accurately categorize pornography.

Visual Object Recognition

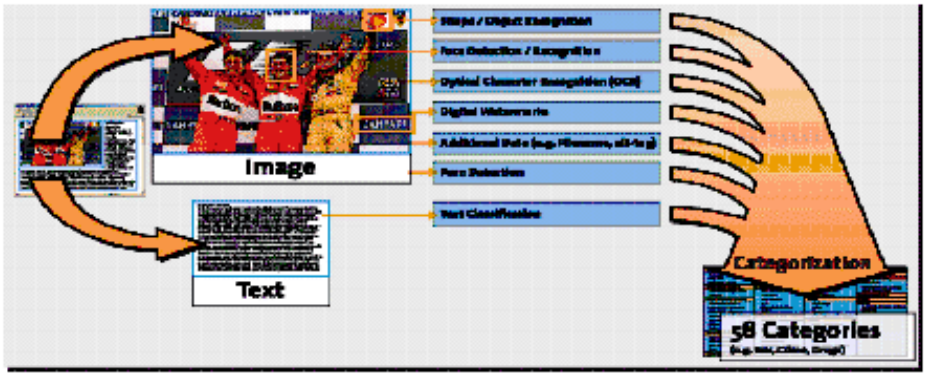
Symbols can be an important indicator for classification in certain categories such hate/discrimination (swastika, etc.) and political parties (logos). As such, the automatic classification process utilizes its powerful image analysis capabilities to identify unique images such as trademarks, logos, symbols, brands and so forth. These are then factored into the overall categorization process.

Visual Optical Character Recognition

As indicated above, a significant amount of textual information in web pages is actually embedded in images. To unlock this information, optical character recognition techniques are applied to all images. When embedded text is found, it is analyzed using the text analysis techniques previously described. Clearly text such as photo titles provide valuable information that can greatly improve the accuracy of categorization.

Overall Classification

To arrive at the final classification an algorithm is used to weigh the results of each analysis technique. This proprietary algorithm has been developed through years of research on millions of web sites, where the accuracy of each technique in appropriately classifying a particular category has been studied. Having a variety of different inputs available allows errors in any particular analysis technique to be corrected by other considerations, resulting in an extremely accurate classification process.



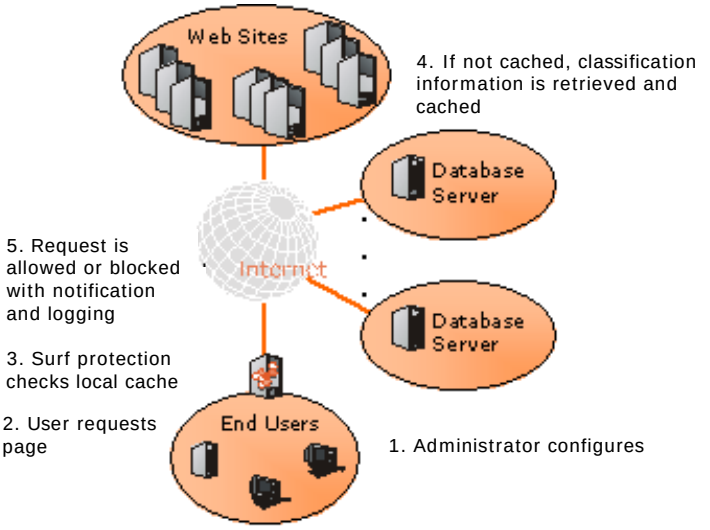
Web Site Categorization Combining Multiple Analysis Techniques

Support for Multiple Languages

The overall crawling and classification process is designed to be completely independent from the language used on a Web site. Only a fraction of the analysis algorithms require language-specific tuning (text classification and visual optical character recognition). For each Web page, language is determined automatically, and language-specific modules are used for text classification. For the training of language-specific modules, linguistic experts currently cover the following languages: English, Spanish, French, German, Portuguese, Italian, Russian, Polish, Chinese, Japanese, Korean, Arabic and Hebrew.

Implementing A Web Filtering Solution

Implementing automated web filtering in your environment can be a straightforward process. In the case of Astaro's implementation, after purchasing the Web Security option available with Astaro Security Gateway, the administrator configures the desired monitoring and blocking policies through a simple point-and-click browser interface. When a user requests a web page, Surf Protection looks up the category of the web page in a locally cached URL database. If the web page belongs to a category that violates established policies, the request is blocked, the user is notified and the incident is logged.



Implementing Web Filtering With Astaro Surf Protection

Surf Protection maintains the local cache, which is a subset of the master database, based on user requests. If a requested page is not locally cached, Surf Protection retrieves the categorization information from one of the geographically distributed database servers containing a copy the master database, and adds it to the local cache. This approach minimizes the amount of downloading required, while ensuring that full protection is maintained.

Integrating Web Filtering Into A Security Architecture

Web filtering is only a single component of an effective perimeter security architecture. A firewall, VPN gateway, network virus protection and spam protection are also deployed in most organizations, with wireless protection, intrusion prevention and other components present in many.

Traditionally organizations have pieced together their perimeter security architecture from individual point solutions, each designed to provide one of the functions listed above. As the number of threats/needs has increased, this approach has become increasingly costly, cumbersome and insecure. Organizations no longer have the staffs or budgets to effectively evaluate, purchase, install, integrate, manage and update this broad array of point solutions. Furthermore, burgeoning integration and update issues are creating highly undesirable security gaps. A more comprehensive approach to the broad and evolving nature of Internet threats is required.

Astaro Security Gateway

Astaro Security Gateway, based on Astaro's award winning Astaro Security Linux, is a comprehensive, integrated security solution that provides complete protection against a multitude of security risks of connecting to the Internet, eliminating the need to piece together point solutions.
The Astaro Security Gateway, available as software or appliance, fully integrates all perimeter security applications required to protect a corporate network in one simple to manage solution:

Email Security

- *Virus Protection for Email* – catches viruses in SMTP and POP3 emails and attachments.
- *Spam Protection* – uses nine different techniques to filter out spam and without stopping legitimate emails.
- *Phishing Protection* –blocks emails from criminals trying to trick users into revealing confidential information.

Web Security

- *Spyware Protection* – detects and blocks spyware infection attempts as well as spyware communication from already infected systems
- *Virus Protection for the Web* – defends computers from virus infections from web downloads and web-based email.
- *Content Filtering (*Surf Protection) – can block Internet access to 60 categories of web sites.

Network Security

- *Firewall* – guards Internet communications traffic in and out of the organization with stateful packet inspection and application-level proxies.
- *Intrusion Protection* – detects and blocks probes and application-based attacks using heuristics, anomaly detection, and pattern-based techniques.
- *Virtual Private Network Gateway* – assures secure communications with remote offices, "road warriors," and telecommuters.

Conclusion

While the web is an extremely powerful tool for all organizations, inappropriate use can negatively impact productivity, the work environment and legal liabilities. Organizations need to put in place policies and enforcement tools to minimize these potential impacts.

Electronic URL blocking has proven to be a successful means of enforcing policies. While there are many different approaches to implementing URL blocking, database-based automated classification techniques have proven to be the most effective in terms performance and accuracy. Astaro Surf Protection utilizes this approach, delivering market-leading results in terms of blocking, overblocking and coverage measurements.

Astaro Surf Protection is an optional component of Astaro Security Gateway. By combining web filtering with firewall, VPN, virus protection, spam protection, and other security functions, Astaro uniquely delivers a solution with much lower total cost of ownership, simplified management and greater security. A free 30-day evaluation version can be downloaded at www.astaro.com to verify operation in your environment.

Appendix A: Astaro Surf Protection URL Database Categories

Nudity

Pornography
Includes websites containing the depiction of sexually explicit activities and erotic content unsuitable to children or persons under the age of 18.

Erotic / Sex
Includes websites containing erotic photography and erotic material, as it can be found on television or obtained from magazines free of charge. Sex toys are also in this category. Sexually explicit activities are not listed here.

Swimwear / Lingerie
Includes websites containing nudity, but with no sexual references. Includes bikini, lingerie and nudity.

Ordering

Online Purchasing
Includes websites with online shops, where there is a possibility to select from a product range and order online.

Auctions / Small Advertisements
Includes websites with online/offline auction sites, auction houses and online/offline advertisements.

Society / Education / Religion

Governmental Organizations
Includes websites with content for which governmental organizations are responsible (e.g. government branches or agencies, police departments, fire departments, hospitals) and supranational government organizations such as the United Nations or the European Community.

Non-Governmental Organizations
Includes websites of non-governmental organizations such as clubs, communities, non-profit organizations and labor unions.

Cities / Regions / Countries
Includes websites with regional information, web sites of cities, regions, countries, city maps and city magazines.

Education / Enlightenment
Includes websites of universities, colleges, public schools, schools, kindergartens, adult education, course offerings, dictionaries and encyclopedias of any topic.

Political Parties
Includes websites of political parties and those sites that provide information about a particular political party.

Religion
Includes websites with religious content, information about the five main religions, and religious communities that have emerged out of these religions.

Sects
Includes websites about sects, cults, psycho-groups, occultism, Satanism etc.

Criminal Activities

Illegal Activities
Includes websites describing illegal activities according to German law, such as instructions for murder, manuals for bomb building, manuals for murder, instructions for illegal activity, child pornography, etc.

Computer Crime
Includes websites describing illegal manipulation of electronic devices, data networks, methods and also password encryption, manuals for virus programming and credit card misuse.

Political Extreme / Hate and Discrimination
Includes websites with extreme right and left-wing groups, sexism, racism and the suppression of minorities.

Hacking / Warez / Illegal Software
Includes websites with software cracks, license key lists and illegal license key generators.

Violence / Extreme

Includes websites that are normally assigned to other categories, but are particularly extreme in their content (e.g. violence).

Games / Gambling

Gambling
Includes websites of lottery organizations, casinos and betting agencies.

Computer Games
Includes websites of computer games, computer game producers, cheat sites and online gaming zones.

Toys
Includes websites containing information about dolls, modeling, scale trains/cars, board games, card games and parlor games, etc.

Entertainment / Culture

Cinema / Television
Includes websites ranging from cinema, television, program information, to video on demand.

Recreational Facilities / Amusement / Theme Parks
Includes websites containing organization for recreational activities, e.g. public swimming pools, zoos, fairs and amusement parks.

Art / Museums / Memorials / Monuments
Includes websites from theatres, museums, exhibitions, and opening days.

Music
Includes websites from radio stations, online radio, MP3, Real Audio, Microsoft Media, homepages of bands, record labels and music vendors.

Literature / Books

Includes websites containing literature such as novels, poems, specialized books, cooking books, advisories and many more.

Humor / Comics

Includes websites with jokes, sketches and other humorous content.

Information / Communication

General News / Newspapers / Magazines

Includes websites that inform about general topics such as youth magazines or newspapers.

Web Mail

Includes websites that enable internet users to send or to receive e-mails via the internet (mailbox). All providers of web mail services are categorized here as well.

Chat

Includes websites that allow users to have a direct exchange of information with another user from place to place. Also listed are chat room providers.

Newsgroups / Bulletin News Boards / Discussion Sites

Includes websites that enable sharing information such as on a pin board, including a variety of topics.

SMS / Mobile Phones Fun Applications

Includes websites that enable users to send short messages via SMS via the internet to a mobile phone. It also includes providers and services for mobile phone accessories that are not necessary for daily use such as games, ring tones and covers.

Digital Postcards

Includes websites that allow people to send digital postcards via the internet, and also the providers of these services.

Search Engines / Web Catalogs / Portals

Includes websites containing search engines, web catalogues and web portals.

IT

Software and Hardware Vendors / Distributors

Includes websites of producers of hardware used for information, measuring and modular technology, vendors of software, and distributors that provide hardware and software.

Communication Services

Includes websites such as web hosting and Internet Service Providers as well as providers of broadband services.

Information Security Sites

Includes websites that inform people about security, privacy, data protection in the Internet and in other broadband services as telecommunications.

Web Site Translation

Includes websites that enable the translation of parts or the entire content of a website into another language.

Anonymous Proxies

Includes websites that allow users to anonymously view websites.

Drugs

Illegal Drugs

Includes websites about illegal drugs such as LSD, heroine, cocaine, XTC, pot, amphetamines, hemp and the utilities for drug use (e.g. water pipes).

Alcohol

Includes websites dealing with alcohol as a pleasurable activity (e.g. wine, beer, liquor, breweries) and the websites of alcohol distributors.

Tobacco

Includes websites about tobacco and smoking (cigarettes, cigars, pipes), and websites of tobacco vendors.

Self Help / Addiction

Includes websites from self-help groups, marriage guidance counseling, and help for addiction problems.

Lifestyle

Dating / Relationship
Includes websites that promote interpersonal relationships.

Restaurant / Bars
Includes websites about bars, restaurants, discotheques, and fast food restaurants.

Travel
Includes websites about monuments, buildings, sights, travel agencies, hotels, resorts, motels, airlines, railways, car rental agencies and tourist information.

Fashion / Cosmetics / Jewelry
Includes websites about fashion, cosmetics, jewelry, perfume, modeling and model agencies.

Sports
Includes websites such as resort sports, fan clubs, events (e.g. Olympic Games, World Championships), sport results, clubs, teams and sporting federations.

Building / Residence / Furniture
Includes websites such as property markets, furniture markets, prefabricated houses, design, etc.

Nature / Environment
Includes websites about pets, market gardens, environmental protection etc.

Private Homepages

Includes private websites and homepage servers.

Job search

Includes websites of job offerings, job searches, job agencies, labor exchanges, temporary work, etc.

Finance / Investing

Investment Brokers / Stocks
Includes websites displaying stock exchanges rates, and deal exclusively with the main stocks like finance, brokerage and online trading.
Financial Services / Investment / Insurance
Includes websites about real estate, insurance, and construction financing.
Banking
Includes websites of resort bank offices, credit unions, and online bank accounts.

Vehicles / Transportation

Includes websites from the resort automobiles, car tuning, car-exhibitions, motorbikes, airplanes, ships, submarines, bikes, railway etc.

Weapons

Includes websites dealing with guns, knives (not including household or pocket knives), air guns, fake guns, explosives, ammunition, military guns (tanks, bazookas), guns for hunting, and swords.

Medicine

Health / Recreation / Nutrition
Includes websites about hospitals, doctors, drugstores, psychology, nursing, health food stores and medicine.
Abortion
Includes websites about abortion.

Spam

Spam URLs
Contains Web Sites that are solicited in spam e-mails
Phishing URLs
Contains Web Sites that are solicited in phishing e-mails

Spyware

Contains Web Sites that install data-transmitting programs without the user's knowledge