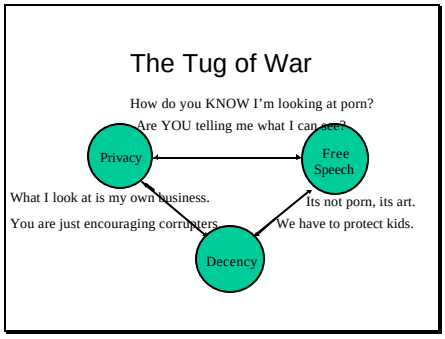
Ethical Issues in Firewall Administration

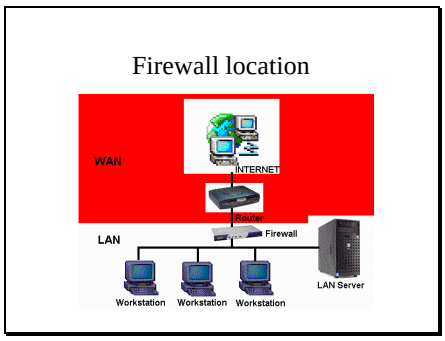
John Bailey
September 5, 2003

For any organization with a Local Area Network, a firewall is essential to prevent unauthorized outsiders from gaining access to information inside that network. While this is the firewall's primary purpose, it has an additional use. While the Internet offers unparalleled access to information, it also contains much material that is objectionable. Some firewalls offer a range of tools for preventing users who are inside the network from gaining access to information on the Internet. Determining how these tools for filtering or blocking websites are to be applied confronts the Local Area Network administration with the ethical challenge of balancing between 1) standards of decency 2) free access to information and 3) individual's rights to privacy.



As the slide shows, this can be viewed as a tug of war between three kinds of people. There are those whose primary concern is their personal information space. They resent intrusion of any kind into their space. There are others who find risqué or lascivicious material offensive and will take aggressive steps to purge their environment of such material. Third, there are those whose main concern is avoiding censorship or any restriction to free access to information. The interplay of these attitudes with the relatively blunt tools available for managing and restricting access to "objectionable material" on the Internet can make the task of administering a firewall quite interesting

A firewall is a specialized computer which connects the Local Area Network to the Wide Area Network. Its software provides for detection of incoming attempts to gain unauthorized access to or control of computers on the Local Area Network. It allows for revising the addresses of all computers on the network, such that they do not appear as valid TCP/IP addresses to the wide area network processes. This is called Network address translation (NAT) and is analogous to having an unlisted phone number. In this case, all stations on the LAN would be "unlisted."



The most powerful capability of a firewall is its ability to refuse to accept packets of data from the WAN which were not requested. Unless a process on a PC within the LAN had requested the information, a packet directed to a PC on the LAN would not be accepted. This can be thought of as analogous to only accepting return calls from numbers previously dialed. "Don't call us, we will call you."

Almost incidental to these fundamental processes for protecting the LAN and its inhabitants is the feature to be discussed in this talk, website blocking.

Website blocking by the firewall is convenient, allowing administration of blocking for the network as a whole rather than separate blocking for each PC on the network. It allows single point control without single point location, since the firewall itself is accessed as web pages on the Local Area Network and can be administered from any location within the LAN. The actions apply, not just to the location but to the entire network.

The tools available for blocking provide the elements from which to construct a strategy

BLOCKING TOOLS.

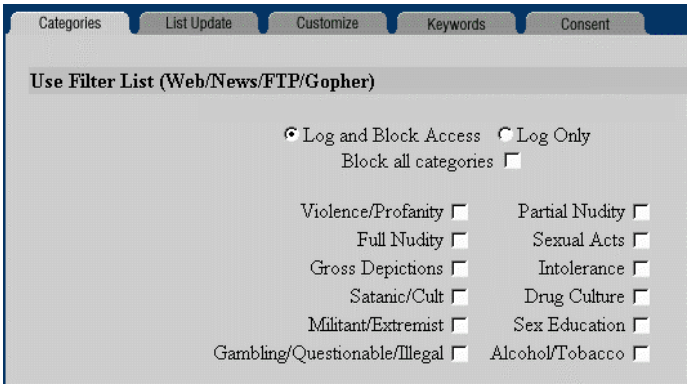
- Subscription blocking list
- Custom blocking list
- Key word blocking
- Email notification of a blocked site
- Logging of blocked sites
- Email log summaries
- Listing of recent site visits

First, there are the options which determine the sites to be blocked--a subscription list, a do-it-yourself custom list, or blocking by key words.

Additionally, there are information gathering features—automatic email notifications and logs which assist the administrator in monitoring the operation.

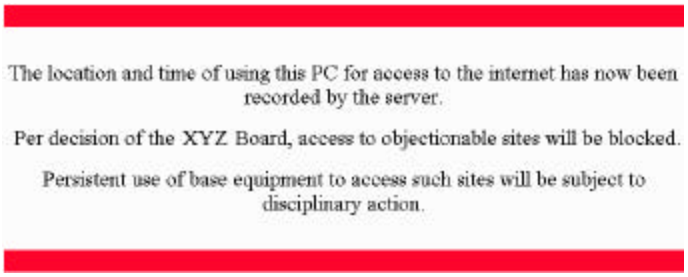
The network administration must choose between key word filtering, commercial blocking list filtering, or customization based on the traffic patterns of its users. Each of these choices has advantages and pitfalls.

Since an organization I support uses SonicWall, a well-known firewall device, our first thought was to subscribe to the SonicWall blocking list. In theory, the process is simple: buy the download from the supplier and click on the categories to be blocked.



This has two disadvantages--not only is the on-going subscription charge high for a small organization, but the blocking is one-size-fits-all. A health oriented organization has users who want access to sites whose content might appear to be objectionable but which actually contain important health information. For example: http://www.menshealth.com, Men's Health Magazine or http://www.arhp.org/ which is the website of the Association of American Reproductive Health professionals. The first of these sites should be blocked. The second arguably should not, but is blocked by some commercial blocking software. (Reference: Kaiser Foundation study) Using a commercial blocking list gives the administrator no simple recourse to access a site that the list supplier has included.

For us, a better alternative is to use customized blocking lists. SonicWall can send email to the administrator when access to a blocked site is attempted by a user. As a result, the administrator can then review usage logs and determine if other unblocked sites were also visited. With this information, as well as times and machines used, it is possible to develop a picture of the usage patterns of offending users and build an impressive private blocking list. With a good starting list, the blocking list grows itself. The problem with this approach is that objectionable sites are never blocked the first time they are visited. The administrator observes a site that is visited, decides it is objectionable and adds it to the blocking list. Thereafter no user can visit that site, getting instead the blocking message.



To overcome the pitfall of always being one visit behind when using custom blocking, we then tried adding key word blocking. Key word blocking may be more trouble than it is worth. Finding keywords which will only show up on objectionable sites but not on acceptable sites is a troublesome process. Key word blocking is useful to eliminate web pages which are named with many variations of the same key core word. Sextracker seems to be a favorite prefix for site names of one collection of objectionable sites. Since there are many variations of the similar name, adding the blocking word "sextracker" allows anticipation of undiscovered and future variations. Using common words as blocking key words simply results in a lot of backtracking as perfectly harmless sites show up as blocked.

The main value of key word blocking is as a supplement to custom blocking. Since key word blocking will easily block sites which are not objectionable, it is perhaps most effective when used in combination with a permissions technique that allows authorized users on certain machines to by-pass blocking, thus eliminating some of the problem of excessive censorship.

Permission pages are intended to inform a user of the organization's internet access policy and what they can expect with regard to monitoring their usage. Some types of permission pages can allow users on authorized machines to elect non-blocking. Depending on the selection a user makes on such a PC, the firewall blocking can be either applied or bypassed, depending on user election. The value of this approach is that much more restrictive blocking can be used for the custom blocking list and key word blocking combination, but certain users can be granted the option of overriding these restrictions.

The disadvantage of this approach is that a LAN web server is required to present the permission screens, thus adding an additional complexity to the administration task.

Another strategy component can be termed "site selection redirection." In some instances, the pattern of usage may lead to the conclusion that objectionable sites are being visited because the user is searching for information but the information suppliers are forcing the objectionable sites on

them. An example of this in a school or library setting might be based on the following logic:

1) Teens know how to use search engines to research questions.

2) They have a natural teenager's curiosity about sex

3) They frame a query about a sexual topic.

4) The porno-pushers deluge them with indecency.

5) Because of the teen-ager's hormones and naiveté, they can get enticed--being presented with aggressively erotic material

Following this logic, one solution might be to offer, as a substitute for the page requested, a suitable page with information corresponding to the original request.

The concern here is that parents may object to sex education being gratuitously introduced to their children without permission. Permission pages, as outlined above might be used to relieve this concern.

An organization should develop its own Internet Access Policy. As far as practical, such a policy codifies the organization's objectives in controlling access to the Internet, what kinds of material are considered objectionable and the actions it will take to insure that its objectives are satisfied. The actions to be taken will likely include a degree of monitoring, requiring a tradeoff of privacy against the need to insure the intended controls are working properly.

Internet Access Policy (example)

•**Statement of intent:**–Computers are provided at the facility for information research, learning, and the enjoyment of members. In this latter use, they are a perk. Members, associates, and their family members who spend time at the facility are encouraged to use computers at the facility for access to the Internet, but not to **objectionable sites**.

In this policy, **objectionable sites** are ones which contain material involving:

- –Full Nudity
- –Gross Depictions
- –Sexual Acts
- –Partial Nudity

•**Implementation**:

- –Access will be blocked using a custom blocking list.
- –Start up message will advise objectionable site visits are a violation.
- –Blocking will be recorded—time and location.
- –Selections will be monitored.
- –Persistent use will result in sanctions.
- –Exceptions will be by appeal only.

The example policy outlined here was developed after examining examples of policies from the web.. The examples found there have a different style. In this case, the intent was to obtain concurrence from the organization's board of directors as to what we wanted to do and how we would do it.

The implementation of an Internet Access Policy calls for plans and actions by a firewall administrator who must select a technical means to filter information, establish filter settings and monitor their effect. The administrator should report back to the governing body of the organization from time to time. Because the entire process involves many sensitive judgments, some on explosive issues, the administrator's best safeguard is a clear set of operational guidelines which will protect the administrator from emotional, reactive decisions by the governing body.

The degree of control, the violation of privacy and infringement on free access to information are in proportion to the extent to which some few individuals push the limits of decency. Rather than impose severe controls on all users, it is better to impose severe penalties on the few violators. This requires knowing to whom the penalties should be applied. Without excessive control and snooping, it is relatively easy to determine when and on which computer an objectionable site is visited. By noting these times and keeping track of the nature of the sites visited, a pattern may emerge. Comparison of the pattern of visits with other data—comings and goings of the possible users, it eventually becomes possible to identify the violator. At that point, direct intervention—confrontation or threat of public embarrassment may be enough. If not, the policy prescribes the formal steps.

There is, of course, a certain degree of ambiguity regarding the character of certain websites. The site www.menshealth.com is a good example. Although Google Safe Search blocks it entirely, some of its pages are acceptable. To a casual glance, Esquire magazine, for example has about the same level of blatant sex. On the other hand, on examining the whole site, there are many quite objectionable pages. Another filtering process available on the web, the publicly available filter at N2H2.com agrees with this assessment.

www.menshealth.com is a site for which I received a request to remove from the blocking list, based on its health and medical content. At this juncture, the Google SafeSearch test was evoked for the first time. Based on the preponderance of pages which Google SafeSearch would block from the site, it remained on the blocking list.

Our policy evolved to this procedure: If the blocking list denies access to sites which are needed for facility business—for example medical information, a request to remove such a site from the blocking list should be made to the VP of Administration. The standard of acceptance for a site will be generally used search software with content filtering, e.g. if Google SafeSearch using strict content blocking blocks the site in question. If it does, removal of such a site from the

organization's blocking list will be done only with approval of the President.

http://cyber.law.harvard.edu/people/edelman/google-safesearch/ gives a critical report of Google's SafeSearch.

The paper: Empirical Analysis of Google SafeSearch Benjamin Edelman - Berkman Center for Internet & Society - Harvard Law School lists some astonishing gaffes found in its evaluation of SafeSearch.

N2H2, the other filtering software available on the web at http://www.n2h2.com/ provides an on-line evaluation and classification of individual websites a user submits to it.

Some experimentation with both of these filters reveals some of their gaps. N2H2 rates whole sites, not pages. It appears that some sites are simply not classified. Google's SafeSearch appears to have no way of detecting the unsuitable nature of images which a page may contain. If a web page uses acceptable words and phrases, but contains pornographic images, SafeSearch may not filter the page. Specifically, while evaluating www.terra.es, Google showed about 1600 pages were acceptable. One of these: titled Exclusive Russian Girls, used moderate words but contained an animated picture illustrating a link. The animated picture was a close-up of a female performing fellatio on a male partner.

Quoting Benjamin Edelman - Berkman Center for Internet & Society - Harvard Law School : "Accurate Internet filtering is an extraordinarily difficult task still well beyond the reach of current algorithms and methods."

Ethical Questions

- What material is objectionable?
- When does monitoring become snooping?
- When does blocking become censorship?
- What evidence is needed to identify a violator?
- What are just penalties for violation?
- What inconvenience for the many is justified to prevent objectionable behavior?

The issues that emerge in determining what and how to block are largely ones of degree. At either extreme, reasonable people would reach common ground. The cases in the middle become contentious.

The range of precedent and variation of the context between businesses, community organizations, libraries and colleges/universities leads to the conclusion that there are no pat answers. Since every organization is different, any strategy should only be adopted after careful review by its responsible authorities of the full spectrum of issues and options.

References:

M. Streb, C. Perkins, FIREWALLS 24 SEVEN Sybex Network Press 2000 ISBN: 0-7821-259-8

SONICWALL SOHO USERS GUIDE, Sonic Wall

B. Edelman, EMPIRICAL ANALYSIS OF GOOGLE SAFESEARCH, http://cyber.law.harvard.edu/people/edelman/

See No Evil: How Internet Filters Affect the Search for Online Health Information. Kaiser Foundation, http://www.kff.org/

Children's Internet Protection Act (CIPA), American Library Association, http://www.ala.org/

The Digital Millennium Copyright Act, The UCLA Online Institute for Cyberspace Law and Policy, http://www.gseis.ucla.edu/iclp/dmca1.htm

INTERNET RESTRICTION AND CENSORSHIP, The Chronicle of Higher Education, http://chronicle.com/infotech/

Ethical Issues in Firewall Administration, St. John Fisher conference on Ethics, October 10-11, 2003– http://home.rochester.rr.com/jbxroads/blocking

Appendix I
generic internet access policy

XXX Organization
Internet Access Policy

Intent:

Computers are provided at the facility for information research, learning, and the enjoyment of members. In this latter use, they are a perk. Members, associates, and their family members who spend time at the facility are encouraged to use computers for access to the Internet, but not to **objectionable sites**.

In this policy, **objectionable sites** are ones which contain material involving:

Violence/Profanity	Partial Nudity
Full Nudity	Sexual Acts
Gross Depictions	Intolerance
Satanic/Cult	Drug Culture
Militant/Extremist	Sex Education
Alcohol/Tobacco	Gambling/Questionable/Illegal Activities

Sites which could incur service charges billed to this organization will be considered objectionable.

Implementation:

- Access to objectionable sites from computers on the facility Local Area Network will be blocked using a custom blocking list.
- All facility computers will display a start up message to advise the user at the start of a web browsing session
    - that the time and location of their use of the web may be logged
    - that access to objectionable sites is a violation of the XXX Organization's Internet Access Policy
- Blocking of known objectionable sites will be recorded for all facility computers.
- Selection of sites by users on facility computers will be monitored to identify sites that should be added to the blocking list.
- Persistent use of facility computers for access to objectionable sites will result in sanctions against the user which may include suspension from the corps or revocation of their privileges of using facility computers or facilities.
- If users systematically circumvent these controls, then only individuals with passworded accounts will be granted access to the Internet, to insure compliance with this policy.
- If the blocking list denies access to sites which are needed for facility business—for example medical information, a request to remove such a site from the blocking list should be made to the VP of Administration. The standard of acceptance for a site will be generally used search software with content filtering, e.g. if Google SafeSearch using **strict content blocking** blocks the site in question. If it does, removal of such a site from the XXX Organization's blocking list will be done only with approval of the President.

Adopted by the Board of Directors of the XXX Organization
Date of adoption