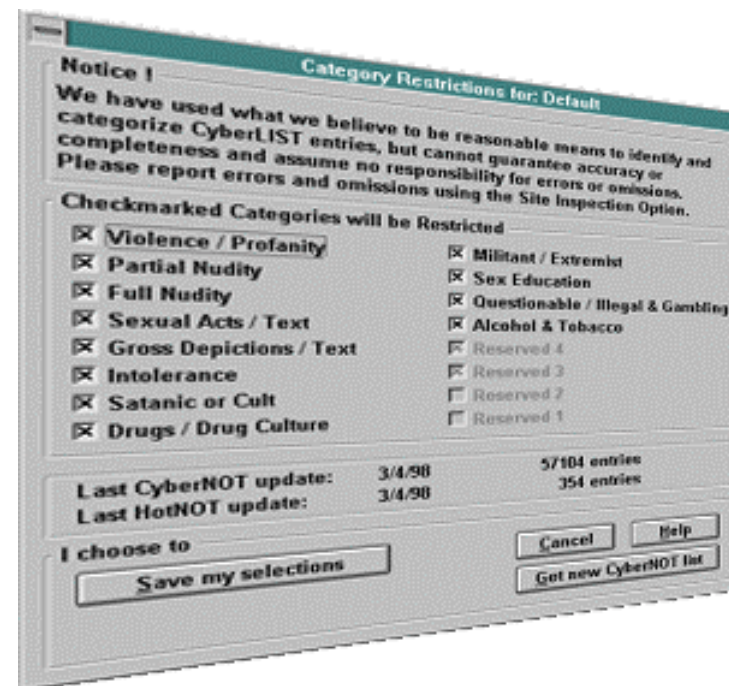


Internet Filtering



Today web browsing accounts for the majority of the traffic both in and out of an Internet connected organization. Businesses and schools need to be able to enforce Internet access policies and control the content accessed from within the organization. The Internet Gateway module includes the ability to create and enforce Internet access policies using the built-in CyberNOT access control feature.



Categories

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

CyberNOT - Subscription Based



The CyberNOT access control feature is provided on an annual subscription basis. Once the activation code is installed the firewall system automatically updates the CyberNOT list on a daily basis and installs a new list on a weekly basis. At the heart of the Internet Gateway module is the CyberNOT List. Professional researchers compile these lists and organize the sites into categories. Sites added to the CyberNOT List meet a set of publicly posted criteria that are reviewed by the CyberNOT Oversight Committee.

How it Works

Any on-line content that contains more than 3 instances in 100 messages or any easily accessible pages with graphics, text or audio that fall within the definition of the categories will be considered sufficient to place the source in that category.

Sites on the CyberNOT List are designated down to the file directory. This means that appropriate material at an Internet address need not be blocked simply because there is some restricted material elsewhere at the address.



For the full detail of the
CyberPatrol CyberNOT
Category list criteria visit
[www.cyberpatrol.com/
product/cyberlists.aspx](http://www.cyberpatrol.com/product/cyberlists.aspx)