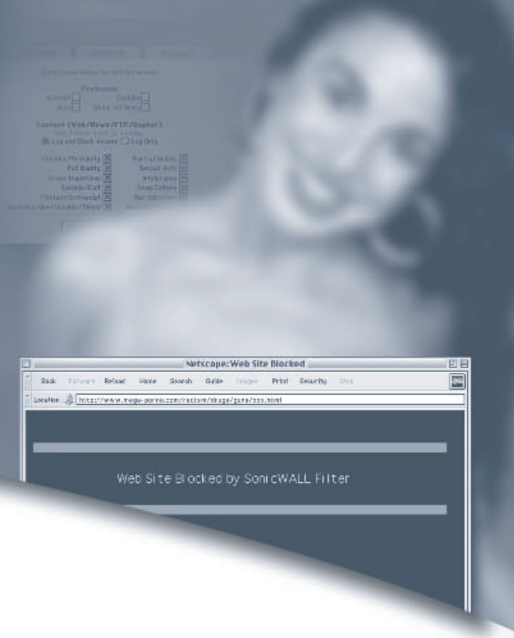
SONICWALL

Internet Content Filtering Overview



Web Site Blocked by SonicWALL Filter

Inappropriate online content can create an uncomfortable work environment, lead to harassment lawsuits, or expose children to pornography or racially intolerant sites. SonicWALL Internet Content Filtering allows organizations to maintain Internet access policies tailored to their specific needs, with built-in support for URL filtering, keyword blocking and cookie, Java and ActiveX blocking.

SonicWALL Content Filtering offers:

- ***Blocking of objectionable Web sites based on the CyberNOT List***
- ***Customizable URL and keyword blocking***
- ***Java, ActiveX and cookie blocking***

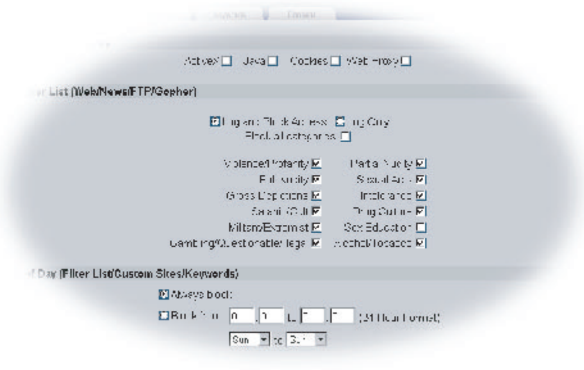
SonicWALL's Internet Content Filter List Subscription is based on the CyberNOT List, a dynamic list of sites containing inappropriate material, which is maintained by Cyber Patrol. This is the same, highly regarded list used by America Online, Media One, AT&T World Net, Bell Atlantic and Microsoft. The SonicWALL Content Filter List provides network administrators with a flexible tool to use in the creation and administration of Acceptable Use Policies.

The Content Filter List allows the administrator to select categories of Internet sites, such as pornography or racial intolerance, to block or monitor access. Automatic weekly updates of the Content Filter List ensure proper enforcement of access restrictions for new and relocated sites. SonicWALL's content filtering can also be customized to add or remove specific URLs from the blocked list, and also to block specific keywords. When a user attempts to access a site that is blocked by the SonicWALL, a customized message is displayed on the user's screen. SonicWALL Internet security appliances can also be configured to log attempts to access sites on the CyberNOT List, custom list, and keyword list. This provides the ability to monitor Internet usage before putting new usage restrictions in place.

SonicWALL Content Filtering Features and Benefits

- **Content Filter List Subscription.** Since content on the Internet is constantly changing, a Content Filter List subscription is available which automatically updates the SonicWALL's Content Filter List on a weekly basis to ensure that access restrictions to new and relocated sites are properly enforced.
- **URL Filtering with Trusted and Forbidden Domains.** Network administrators can specify domains or hosts (e.g., "yahoo.com) that access can be allowed ("Trusted") or denied ("Forbidden"). This feature can be used to customize the Content Filter List, or to allow Web access to sites on a custom list. With careful screening, this can be close to 100% effective at blocking objectionable material.
- **Keyword Blocking.** SonicWALL Internet security appliances can optionally scan both the filename field and host field for specific keywords, and block any requests that contain them. For example, if the administrator enters the keyword "sex," access to sites such as http://www.hotsex.com will be blocked.
- **Java, ActiveX and Cookie Blocking.** Java and ActiveX scripts are often used for hacker attacks. "Cookies," which direct a remote Web browser to save small amounts of data on its local hard disk, can be used to store preference information, and track Web usage history. For this reason, they can cause some privacy concerns. SonicWALL may be configured to block Java and ActiveX scripts, as well as Cookies.
- **Block by Time of Day.** SonicWALL Internet security appliances allow the network administrator to make filtering active only during certain times of day. A school could, for example, have filtering on during school hours and then remove filtering controls after school. A business could allow unfiltered Internet access to employees during a lunch hour and after work hours. When Time of Day filtering is activated, all filtering functions (filter list, cookie blocking, keyword blocking, etc.) will be on or off during specified times.

SonicWALL Internet security appliances utilize the CyberNOT List to block access to sites, which have been classified in one of the following categories:



ActiveX ☐ Java ☐ Cookies ☐ Web Proxy ☐

List (Web/News/FTP/Gopher)

☒ Log and Block Access ☐ Log Only
Block all categories ☐

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

Day (Filter List/Custom Sites/Keywords)

☒ Always block
☐ Block from 0 : 0 to : (24 Hour format)
Sun to Sat

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

Content Filter List Part Numbers

01-SSC-2733 Content Filter List 1 Year Subscription - For SonicWALL TELE2
01-SSC-2560 Content Filter List 1 Year Subscription - For SonicWALL SOHO2 10-User
01-SSC-2563 Content Filter List 1 Year Subscription - For SonicWALL SOHO2 50-User
01-SSC-2566 Content Filter List 1 Year Subscription - For SonicWALL XPRS2, SonicWALL PRO and PRO-VX